SBC Core

Release Notes

Software Release: 09.02.03R002
Document Revision: 01.01
Published: 19 November 2021

Copyright

Disclaimer and Restrictions

The publication is for information purposes only and is subject to change without notice. This publication does not constitute a commitment on the part of Ribbon. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Ribbon assumes no liability resulting from technical or editorial errors or omissions, or for any damages whatsoever resulting from the furnishing, performance, or use of the information contained herein. Ribbon reserves the right to make changes to this publication and to Ribbon products without notice in its sole discretion. This publication is not meant to define any interfaces between Ribbon products and any third-party hardware or software products.

Warranties

THIS INFORMATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT SHALL THE RIBBON BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR PERFORMANCE OF THIS INFORMATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Compliance with Applicable Laws and Export Control Laws

The information in this publication is subject to all applicable U.S. federal, state, and local laws. The customer use, distribution, and transfer of any technical information shall be in compliance with all applicable export and import laws and regulations. All Ribbon products and publications are commercial in nature; and the use, duplication, or disclosure by the United States Government is subject to the restrictions set forth in DFARS 252.227-7013 and FAR 52.227-19.

Trademarks

The trademarks, logos, service marks, trade names, and trade dress (“look and feel”) on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

UNCONTROLLED COPY: The master of this content is stored in an electronic database and is “write protected”; it may be altered only by authorized persons. While copies may be printed, it is not recommended. Viewing of the master electronically ensures access to the current content. Any hardcopies taken must be regarded as uncontrolled copies.

For access to the technical documentation, log in through the Ribbon Support Services website at
https://ribboncommunications.com/services/support-services/technical-documentation

SBC Core 09.02.03R002 Release Notes

Table of Contents

About SBC Release Notes

This release note describes new features, the latest hardware and software requirements, known limitations and other pertinent release information for the latest release of SBC Core.

Please note that all Ribbon bugs reported by customers on a given software release will be fixed in the latest release on that software release branch.

To view and download the latest End of Product Sale (EoPS) and other End Of Life (EOL) notices, navigate to the Resource Library on the corporate website (https://ribboncommunications.com/company/get-help/resource-library).

Release Notes Use and Distribution

Associated Ribbon Announcements

The following Ribbon announcements (formerly known as WBAs) are referenced in this release note:

- **Warning-14-00020748**: Verify system and databases are fully in sync prior to Live Software Upgrade (LSWU). Applies to all SBC platforms (HW, SWe, Cloud) except the SBCs deployed in a Distributed SBC (D-SBC) architecture
- **Warning-21-00029858**: The AWS SBC Might Fail to Come Up Due to a Metadata Query Failure from the Metadata Server.
- **Warning-21-00029859**: Policy Data syncInProgress after Upgrade Revert
- **Warning-21-00029843**: Unable to Access SBC EMA and PM Post LSWU due to server.key File Corruption

To view/download Ribbon announcements, do the following:

1. Log on to the Ribbon Support Portal (https://ribboncommunications.com/services/ribbon-support-portal-login).
2. From the Quick Access menu, click and download the "Ribbon Support Portal User Guide", and navigate to the "ANNOUNCEMENTS tab" section for instructions to search for and view announcements.

Problems or Questions

For problems or questions, contact the Global Support Assistance Center:

Ribbon Support Portal: https://ribboncommunications.com/services/ribbon-support-portal

Voice: +1-833-RIBBON1 (1-833-742-2661)

About SBC Core

The SBC Core platforms address the next-generation needs of SIP communications by delivering media transcoding, robust security and advanced call routing in a high-performance, 2RU, and 5RU form-factor devices enabling service providers and enterprises to quickly and securely enhance their network by implementing services like SIP trunking, secure Unified Communications and Voice over IP (VoIP).

For more product information, refer to the section About SBC Core in the main documentation space.

Interoperability

The SBC Core software interoperates with the following:

- SIP/H.323 compliant IADs and IP-PBXs
- PSX Policy Server Softswitch via SIP redirects and/or Diameter+ protocol
- SBC 9000 through SIP call signaling and Networks MCS protocol

H.323-SIP and SIP-H323 Calls

When using H.323-SIP and SIP-H.323 call flows, an additional Re-invite/Update may get generated towards the SIP side. To suppress this, enable the IP Signaling Profile (IPSP) flag `Minimize Relaying Of Media Changes From Other Call Leg` at the SIP side.

- For CLI IPSP flag details, refer to Flags - CLI.
- For EMA IPSP flag details, refer to Common Ip Attributes - Flags.

Note
H.323 is not supported on SBC SWe cloud deployments.

Compatibility with Ribbon Products

Tip
When upgrading your network, ensure to upgrade each product to the most current release to take advantage of the latest features, enhancements, and fixes.

Info
For complete interoperability details between various Ribbon products, including backwards compatibility, refer to Ribbon Product Compatibilities.

Refer to SBC 5000-7000-SWe Interoperability Matrix for the latest and minimum compatible product versions supporting this release.

New Features

New Features in Release 09.02.03R002

There are no new features in this release.

New Features in Previous Releases

To view features in previous releases, refer to the following release notes:

- SBC Core 09.02.03R000 Release Notes
- SBC Core 09.02.02R002 Release Notes
- SBC Core 09.02.02R001 Release Notes
- SBC Core 09.02.01R000 Release Notes
- SBC Core 09.02.00R001 Release Notes

Sample Heat Templates Included in This Release

To instantiate the SBC instances, the following templates can be used:

Table 1: SBC Heat Templates

Template Name	Description
heatRgNoDhcp.yaml	Used to instantiate no DHCP, IPv4 or IPv6 deployments. The template supports I-SBC, M-SBC, S-SBC, MRFP and SLB node types. This template includes instructions to enable port redundancy.
heatOamNoDhcp.yaml	Used to instantiate an OAM node.
heatRgNoDhcp-TSBC-template.yaml	Used to instantiate a T-SBC node.

Note
Example template files are packaged together in .tar.gz and .sha256 files separate from the SBC Core application installation and upgrade files:

- cloudTemplates.tar.gz
- cloudTemplates.tar.gz.sha256

SBC SWe Cloud Requirements for OpenStack

The system hosting the SBC SWe Cloud must meet the below requirements for OpenStack:

Table 2: Server Hardware Requirements

Configuration	Requirement
Processor	Intel Xeon processors (Nehalem micro-architecture or above) with 6 cores and above (processors should support hyper-threading). **Note** Ribbon recommends Westmere (or newer) processors for better SRTP performance. These processors have the AES-NI instruction set for performing cryptographic operations in hardware.
RAM	Minimum 24 GiB
Hard Disk	Minimum 100 GB

Network Interface Cards (NICs)	Minimum 4 NICs. **Note** Make sure NICs have multi-queue support which enhances network performance by allowing RX and TX queues to scale with the number of CPUs on multi-processor systems. **Note** The Intel I350, x540, x550, and 82599 Ethernet adapters are supported for configuring as SR-IOV and DirectPath I/O pass-through devices. **Note** The PKT ports must be 10 Gbps SR-IOV enabled ports. **Note** 6 NICs are required to support PKT port redundancy.

The system hosting the SBC SWe must meet the following requirements to achieve the performance targets listed:

Table 3: S-SBC SWe Requirement

S-SBC SWe Requirements for 1000 CPS/120K Signaling Sessions	Notes
32 vCPUs	Due to the workload characteristics, allocate 20 physical cores with two hyper-threaded CPUs from each core to the SBC.
128 GiB RAM	Must be Huge Page memory. The minimum page size is 2048 KiB, but 1048576 is recommended.
100 GB Disk	None
4 vNICs/6 vNICs	Attach MGT0 port to the Management VirtIO Tenant network. HA port has to be on IPv4 VirtIO Tenant network. Attach PKT0 and PKT1 ports to SR-IOV and Provider network. You must have 6 vNICs to enable PKT port redundancy. For more information, refer to the SBC SWe Features Guide.

Table 4: M-SBC SWe Requirement

M-SBC SWe Requirements for 40K Media Sessions	Notes
16 vCPUs	Due to the workload characteristics, allocate 10 physical cores with two hyper-threaded CPUs from each core and from single NUMA node to the SBC.
32 GiB RAM	Must be Huge Page memory. The minimum page size is 2048 KiB, but 1048576 is recommended.
100 GB Disk	None

4 vNICs/ 6 vNICs	Attach MGT0 port to the Management VirtIO Tenant network. HA port has to be on IPv4 VirtIO Tenant network. Attach PKT0 and PKT1 ports to SR-IOV and Provider network. You must have 6 vNICs to enable PKT port redundancy. For more information, refer to the SBC SWe Features Guide.

Note
All NIC ports must come from the same NUMA node from which the M-SBC SWe instance is hosted.

OpenStack Requirements

The SBC SWe supports the following OpenStack environments:

- **Newton** with RHOSP 10 and RHEL 7.4
- **Queens** with RHOSP 13 and RHEL 7.5

Note
The SBC SWe was tested on OpenStack Queens with RHOSP 13 and RHEL 7.5.

SBC SWe Requirements for KVM

The following table lists the server hardware requirements.

Table 5: KVM Hypervisor Server Hardware Requirements

Configuration	Requirement
Processor	Intel Xeon processors (Nehalem micro-architecture or above) with 6 cores and above (processors should support hyper threading). **Note** Ribbon recommends using Westmere (or newer) processors for better SRTP performance. These processors have the AES-NI instruction set for performing cryptographic operations in hardware. **Note** The supported CPU Family number is 6 and CPU Model number must be newer than 26. Refer to the Intel Architecture and Processor Identification document for more information.
RAM	Minimum 24 GB
Hard Disk	Minimum 500 GB
Network Interface Cards (NICs)	Minimum 4 NICs **Note** Make sure NICs have multi-queue support which enhances network performance by allowing RX and TX queues to scale with the number of CPUs on multi-processor systems. **Note** The Intel I350, x540, x550, x710, and 82599 Ethernet adapters are supported for configuring as SR-IOV and DirectPath I/O pass-through devices.
Ports	Number of ports allowed: • 2 Management ports. For more information on the second Management port, refer to Second Management Port for SWe Deployed on KVM Hypervisor. • 1 HA port • 2 Media ports

SBC SWe Requirements for VMware

The following table lists the server hardware requirements:

SBC SWe for VMware – Server Hardware Requirements

Configuration	Requirement
Processor	Intel Xeon processors (Nehalem micro-architecture or above) with 6 cores and above (processors should support hyper threading). **Note** Ribbon recommends using Westmere (or newer) processors for better SRTP performance. These processors have the AES-NI instruction set for performing cryptographic operations in hardware. **Note** The supported CPU Family number is 6 and CPU Model number must be newer than 26. Refer to the Intel Architecture and Processor Identification document for more information. **Note** ESXi 6.5 and later releases require approximately 2 physical cores to be set aside for hypervisor functionality. The number of VMs which can be hosted on a server must be planned for accordingly.
RAM	Minimum 24 GB
Hard Disk	Minimum 500 GB
Network Interface Cards (NICs)	Minimum 4 NICs, if physical NIC redundancy is not required. **Note** Make sure NICs have multi-queue support which enhances network performance by allowing RX and TX queues to scale with the number of CPUs on multi-processor systems. **Note** • The following NICs are supported for configuring as SR-IOV and DirectPath I/O pass-through devices. SR-IOV is supported only with 10 Gbps interfaces (x540/82599/x710): Intel I350, x540, x550, x710 and 82599, Mellanox Connect - 4x, Mellanox Connect - 5x, and CISCO VIC. • The VMware Enterprise Plus license is required for SR-IOV.
Ports	Number of ports allowed: • 2 Management ports. For more information on the second Management port, refer to Second Management Port for SWe Deployed in VMware. • 1 HA port • 2 Media Ports (no port-redundancy) • 4 Media ports (with port-redundancy)

Requirements for Using the Infrastructure as Code Environment with SBC SWe

The following tarball file is required to use the IaC environment to deploy SWe N:1 deployments on VMware:

- raf-20.12-iac1.0_sustaining-240.tar.gz

The environment in which you place and expand the IaC tarball must include:

- A Linux server running RedHat Enterprise Linux (RHEL), CentOS 7 or Debian 9
- Python 2.7 or later
- An internet connection for downloading and installing additional files that may be required for your deployment
- Root access on the instance or ability to become root (for example, using sudo su -)
- Access to the vSphere ESXi host IP from the Linux server where the IaC environment is set up.

For more information on IaC, refer to Using the Ribbon IaC Environment to Deploy SBC SWe on VMware.

Required Software and Firmware Versions

The following SBC 51x0/52x0, SBC 5400 and SBC 7000 software and firmware versions are required for this release. For 5xx0, the BIOS is installed during application installation; whereas, for 5400 and 7000, the BMC/BIOS is included in the firmware package and installed during the firmware upgrade.

Table 6: Required Software and Firmware Versions

Components	Software/Firmware	Version
SBC Platform	SBC 51x0/52x0 BMC	V03.22.00-R000
		Kernel: 3.10.108 Busybox: v1.27.2 Openssh: 7.9p1 Openssl: 1.0.2n Lighttpd: 1.4.48-r0 Qualys security issues Password encryption method is SHA512 Lighttpd is secured and supports only TLS1.2 cipher.
	SBC 51x0/52x0 BIOS	V2.7.0
	SBC 5400 Firmware	BMC: V03.22.00-R000 BIOS: V1.18.0
	SBC 7000 Firmware	BMC: V03.22.00-R000 BIOS: V2.14.0
SBC Application	Operating System (OS) Version	V08.02.03-R002
	SonusDB	V09.02.03-R002
	SBC Application	V09.02.03-R002

Note
The firmware package of SBC 5400 and 7000 series includes BMC, BIOS, and other binaries. The firmware is upgraded from the BMC.

How to Verify Currently Installed Software/Firmware Versions

Use the EMA to verify the currently installed software and firmware versions.

Log on to the EMA, and from the main screen navigate to **Monitoring** > **Dashboard** > System and Software Info.

Software Bundles

The following software release bundles are available for download from the Customer Portal:

- SBC5x7x_9.2
- SBCSWe_9.2

Download the appropriate software packages for your desired configuration from the Customer Portal (https://ribboncommunications.com/services/ribbon-support-portal-login) to your PC:

Note
When upgrading from release 9.0 and above, upload the SHA256 checksum file. Otherwise, use the MD5 file.

SBC 5000 Series (51x0/52x0) Firmware

- firmware-5XX0-V03.22.00-R000.img
- firmware-5XX0-V03.22.00-R000.img.md5
- bmc5X00_v3.22.0-R0.rom.md5sum
- bmc5X00_v3.22.0-R0.rom

SBC 5400 Firmware

- firmware-5400-V03.22.00-R000.img
- firmware-5400-V03.22.00-R000.img.md5

SBC 7000 Series Firmware

- firmware-7X00-V03.22.00-R000.img
- firmware-7X00-V03.22.00-R000.img.md5

Note
Execute the Method Of Procedure (MOP) only for upgrading the FPGA image of an SBC 7000 DSP-LC card when the SBC 7000 DSP-LC FPGA version is 0x14. The MOP can be applied at any version time, with the only restriction being that the BMC firmware version is at least 1.25.0. However, if the SBC application is running version V05.01.00R000 or higher, then the DSPs will be set to disabled and transcoding and transrating calls will fail if the SBC 7000 DSP-LC FPGA version is 0x14. Therefore, it is necessary to upgrade the SBC 7000 DSP-LC FPGA if the version is 0x14, before upgrading the SBC to 5.1.0. However, the MOP can be applied if the application version is higher than 5.1.0. Click Here to view the 550-06210_DSP-LC_FPGA_Upgrade_MOP.

SBC Core Operating System Installation Package

The ConnexIP Operating System installation package for SBC Core:

- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.iso
- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.iso.sha256
- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.iso.md5

Note
Once the ConnexIP ISO procedure is completed, the SBC application package is automatically uploaded to SBC platforms.

Release 9.2 OS Patches
Release 9.2 includes a new set of OS security patches, and also a new version of confD. Release 9.2.1 includes a new set of OS security patches including the fix for CVE-2021-3156: Heap-Based Buffer Overflow in Sudo (Baron Samedit).

SBC Core Application Package

The SBC Application installation and upgrade package for SBC Core:

- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.qcow2
- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.qcow2.sha256
- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.qcow2.md5
- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.ova
- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.ova.sha256
- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.ova.md5
- sbc-V09.02.03-R002.x86_64.tar.gz
- sbc-V09.02.03-R002.x86_64.sha256
- sbc-V09.02.03-R002.x86_64.md5
- sbc-V09.02.03-R002.x86_64.signature

For detailed information on installation and upgrade procedures, refer to SBC Core Software Installation and Upgrade Guide.

Cloud Service Archive (CSAR) Packages for VNFM Deployment on OpenStack

These files are for SBC SWe deployments in the OpenStack cloud using VNFM.

For VNFM deployment, the VNF Descriptor (VNFD) file is provided in a Cloud Service Archive (CSAR) package for the type of SBC cluster being deploying. VNFs are independent and CSAR definitions are imported into the VNFM via an Onboarding mechanism. There is a procedure for producing the required CSAR variant, for different personalities (S-SBC, M-SBC), different interface types (virtio, sriov).

Files required for CSAR creation:

- createVnfmCsar.py
- vnfmSol001VnfdTemplate.yaml
- sbc-V09.02.03R002-connexip-os_08.02.03-R002_11_amd64.qcow2

For detailed information on installation and upgrade procedures, refer to SBC Core Software Installation and Upgrade Guide.

For details on CSAR creation, refer to Creating a CSAR Package File.

Upgrade Notes

Warning
A LSWU on an SBC 7000 should only be performed when the total number of active calls on the system is below 18,000. If the criteria is not met, a double failure during the upgrade may occur, thereby losing all active calls. If such a failure occurs, both active and standby SBC services will go down. Contact Ribbon Support immediately.

Warning
Customers upgrading from 922R1 using VMware or KVM need to run the following command as root user on both the active and standby instances:

touch /opt/sonus/conf/swe/capacityEstimates/.indexMarker

This is not required for upgrades from earlier releases.

Note
This note is only applicable for SBC N:1 mode running on virtualized platforms like KVM, VMware. Before beginning the upgrade to 9.2.2R1, issue the following commands on OAM, and then save the configuration to the EMS. This is needed because from 9.2.1R2 release onwards, NTP and timezone settings provided during the deployment will be applied during the system boot-up, and to avoid overwriting those settings by the default NTP and timezone values which are stored in config, you must update the NTP and timezone settings in CDB before the upgrade and save the configuration to the EMS.

```
set system ntp serverAdmin 169.xxx.xxx.x state disabled

commit

set system ntp serverAdmin <ntp_server_ip> version version4 minPoll 4 maxPoll 10

commit

set system ntp serverAdmin <ntp_server_ip> state enabled

commit

set system ntp timeZone vsbcSystem zone <timezone_value>

commit
```

where

<ntp_server_ip> is the IP address for NTP server.

<timezone_value> is the timezone value you must set for the system.

Note
Once the installation or upgrade completes on the SBC 51x0 and SBC SWe platforms, the copy of the installation package (SBC Core Installation and Upgrade Package) is automatically removed from the system.

Note
Release 9.2 and later requires additional user account security practices for SBC SWe deployments in Openstack cloud environments. During upgrade of SBC SWe cloud instances deployed using Heat templates, you must use a template that includes SSH keys or passwords for the admin and linuxadmin accounts. The example Heat templates have been updated to include information on how to specify this type of data in the userdata section of a template.

Note
As an SBC Core password security enhancement, user passwords automatically expire after upgrading to 8.0.x. As a result, users are required to change their passwords upon initial login immediately following the upgrade.

Note
Customers using network licensing mode will be converted to node locked mode (formerly legacy mode) after upgrade to the SBC 8.0.0 Release.

Note
The SBC 8.0 5xx0 and 7000 platforms may exhibit a 7% degradation of CPU performance relative to earlier releases. This is attributable to the Spectre/Meltdown security patches.

Note
In order to take advantage of performance improvements due to hyper-threading refer to the following MOP to increase the number of vCPUs prior to SBC SWe (KVM Hypervisor or VMware) upgrades from pre-07.01.00R000 release to 07.01.00R000 or higher.

Note
In the case of a Live Software Upgrade (LSWU) from 6.0.0R000/6.0.0R001/6.0.0F001/6.0.0F002 to 8.0, The action “Perform Pre-Upgrade Checks” from PM is not supported. Please contact Ribbon Support.

Note
The number of rules across SMM profiles in a system is limited to 10000, and the number of actions across profiles in a system is limited to 50000.

Ensure the above conditions are met before LSWU.

Note
In NFV environments, the method used for upgrades involves rebuilding the instance, which requires additional disk space on the host. The minimum disk space needed for this operation is listed in the table below.

Table 7: Disk Space Requirements

Flavor	Extra Space Required (GB)
S-SBC	80
M-SBC	80
PSX-M	360
PSX-S	360
PSX-Test	360
EMS_SA	150

Note
The SBC 51xx and 52xx systems require 24GB of RAM to run 6.x code or higher.

Note
SWe SBC software enforces I-SBC instances to run only with a single vNUMA node in order to achieve deterministic performance. SWe SBC VM having >8 vCPUs hosted on dual-socket physical server with VMware ESXi software needs to follow the steps below to correct vNUMA topology before upgrading to latest SWe SBC software:

- Check 'numa.nodeAffinity' settings on VM. It should be either 0 or 1 based on which NUMA node PKT ports are connected. The following command on ESXi host can be used to check PKT port NUMA affinity:

```
vsish -e get /net/pNics/<PKT port name - vmnicX>/properties | grep "NUMA"
```

If any of the above settings requires modification, follow the steps below on SWe SBC HA system:

- Shutdown the standby instance.
- If 'numa.nodeAffinity' settings are missing, add the following rows:

numa.autosize.once = FALSE

numa.nodeAffinity' = 0 or 1 (based on PKT port NIC affinity)

On ESXi 6.5 and above releases, vSphere web client can be used to add above rows under Edit settings > VM options > configuration parameters > add parameters;

On ESXi 6.0 and below releases, it can be added under Edit > Advanced > general > configuration parameters > add rows using vSphere client.

- Power-on standby instance.
- Once standby instance is up and running, do manual switchover through CLI and repeat above steps to modify 'number of virtual sockets' , 'numa.nodeAffinity' and 'numa.autosize.once' settings.

For more information, refer to:

- Create a VM
- Creating Virtual Machines using SR-IOV Interfaces
- Creating a New SBC SWe VM Instance with Direct IO Passthru

Note
Before beginning the upgrade on a SBC running code prior to 8.2R0, the following commands on all the DNS Groups needs to be issued if "ednsSupport" is enabled.

Failure statistics are not being mirrored correctly, and the LSWU state may stay in "syncing" if the "ednsFailures " count is non-zero.

1. Issue the following CLI command to clear the EDNS statistics for all DNS Groups in the system.

admin@PLUM> request addressContext default dnsGroup DnsGrp dnsServerReset
reason DNS Server statistics are Reset
[ok][2020-11-06 04:08:13]
admin@PLUM> show status addressContext default dnsGroup DnsGrp
dnsServerStatistics 2

{ ipAddress 10.xx.xx.xx; queries 0; timeouts 0; errors 0; referrals 0; totalTcpConnection 0; tcpConnectionFailed 0; tcpConnectionSuccess 0; tcpConnectiontorndown 0; tcpFallback 0; ednsStatus supported; **ednsFailures 0**; }

[ok][2020-11-06 04:08:22]
admin@PLUM>

2. Disable the ednsSupport to stop mirroring of the statistics if the error count is constantly incrementing or likely to increase during the upgrade.

set addressContext default dnsGroup DnsGrp ednsSupport disabled

Note: The ednsServer stats will be lost/reset during the upgrade.

Note
If the TRF/MRB Features are configured and enabled – some calls are unable to be cleared post upgrade if using the TRF/MRB attributes.

The upgrade is successful and calls continue but some calls may fail to clean up release post upgrade. Session KeepAlive and RTP Inactivity functions will clean any stale calls.

Enable the sessionKeepalive or rtpInactivity monitoring to ensure that mirrored calls are cleaned up post upgrade.

set addressContext default zone ZONE_AS sipTrunkGroup TG_AS_SIPP signaling timers sessionKeepalive <value>

OR

set system media mediaPeerInactivity <value>

set profiles media packetServiceProfile DEFAULT peerAbsenceAction peerAbsenceTrapAndDisconnect

Note
Upgrade from a pre 8.0 release with globalization support for registration enabled will see a registration drop during an upgrade.

If the following localNumberSupport is enabled, those registrations will be dropped after first switchover during LSWU.

% set addressContext <name> zone <name> sipTrunkGroup <name> signaling localNumberSupport <disabled | enabled>

09.02.03R002 Upgrade Information

Warning
Prior to performing an upgrade to this release, you must remove usernames that do not conform to the SBC user-naming rules to prevent upgrade failure. Upgrade can proceed successfully after removing all invalid usernames. The following user-naming rules apply:

- Usernames can begin with A-Z a-z _ only.
- Usernames cannot start with a period, dash, or digit.
- Usernames can contain a period(.), dash(-), alphabetic characters, digits, or underscore(_).
- Usernames cannot consist of digits only.
- Usernames can contain a maximum of 23 characters.

The following names are not allowed:

tty disk kmem dialout fax voice cdrom floppy tape sudo audio dip src utmp video sasl plugdev staff users nogroup i2c dba operator

Note: Any CLI usernames consisting of digits only or not conforming to new user naming rules will be removed after performing a restore config in release 9.2.3R002.

Warning
Prior to performing an upgrade to the 9.x release, the dnsGroups with type mgmt must be specified/updated with the "interface" field. The steps are included in announcement "W-17-00022847".
If the above MOP is not run, the LSWU process may fail because of duplicate trunk group or zone names.

Warning
Prior to performing an upgrade to 9.x release, the duplicate trunk groups or zones must be removed. The steps are included in announcement "W-17-00022689".

If you are upgrading from any SBC version with ePSX configuration to this release, execute the Method of Procedure, MOP to Reconfigure SBC (with ePSX) to External PSX Prior to an Upgrade to 06.00.00R000 Release prior to performing an upgrade. For a list of supported LSWU paths, refer to Supported Upgrade Paths.

SBC SWe Pre-Upgrade Requirements

VM CPU resource allocation requirements

CPU resource allocation requirements for SBC SWe VM are strictly enforced. You must review and verify these VM settings (including co-hosted VMs) against the documented "VM Configuration Recommendations" on the For VMware page in the Hardware and Software Requirements secti on before upgrading.

If you encounter a problem, correct the CPU reservation settings as specified in step 6 of the "Adjust Resource Allocations" procedure on Creating a New SBC SWe VM Instance with VMXNET3:

> ⚠ Set the CPU reservation for the VM so that it equals the physical processor CPU speed, multiplied by the number of vCPUs divided by two.
>
> For example, a configuration of 4 vCPUs with a processor of 2.99 GHz CPU speed, reserve: 2992 * 4/2 = 5984 MHz

If the VM uses the same number of vCPUs as the number of physical processors on the server, this reservation may not be possible. In this case, reduce the number of vCPUs assigned to VM by **one** and set the CPU reservation to the appropriate value.

When using the `show table system serverSoftwareUpgradeStatus` command during the upgrade, the Standby server's LSWU status will always display "Upgrading" even though the upgrade may have failed due to **host checker validation**. To check if host validation failed for the Standby, check for **HostCheck Validation Failed** message in the `upgrade.out` log.

Disable Call Trace feature prior to LSWU/upgrade

As a prerequisite for SWe LSWU/upgrade, disable the Call Trace feature prior to performing the LSWU/upgrade and re-enable it once the LSWU /upgrade is completed.

Manually check for Hostcheck Validation Failed message

Perform the following procedure on the Standby to check for the **Hostcheck Validation Failed** message in the `upgrade.out` log.

1. Log on to **ESXi** of the Standby SBC SWe.
2. Check in `/opt/sonus/staging/upgrade.out` (this log shows the **Hostcheck Validation Failed** error).
3. Power off the VM.
4. Reduce the number of vCPUs assigned to VM by **one** and set the CPU reservation to the appropriate value.
5. Power on the VM. The SBC SWe successfully upgrades to the latest version 6.2.0.
6. Run the command `show table system serverSoftwareUpgradeStatus` to confirm the successful upgrade.
7. Perform similar procedure for LSWU on Active.

Preparing for Upgrade (All Platforms)

Note
The SBC 8.0 release skips the SRV query if the flag in a DNS NAPTR response from the DNS server indicates to proceed with "A" record query as per RFC 2915/3403. This is a change in behavior from previous releases, where the SBC performed SRV queries irrespective of the "flag" setting returned by DNS Server. If you use DNS NAPTR/SRV/A record query from SBC to determine peer transport address, ensure the DNS Server is configured to return ‘S’ flag to invoke an SRV query.

Note
In this release, LSWU infrastructure is added to the Platform Manager (PM), providing the ability to perform LSWU upgrades to later releases using the PM. However, this feature is not currently supported in 4.2.x releases and should not be used at this time.

Warning
Customers who are using the SBC to interop with MS Teams need to review and compare their configuration against the latest configuration guide especially the SMM as it might result in call failures after upgrade if the older SMM is left in place. For more information, refer to SBC 9.2 - MS Teams Solution Guide.

Supported Live Software Upgrade (LSWU) Paths

Attention
This release includes all bug fixes implemented in the releases which are documented in the Supported Upgrade Paths table of this release note.

To view bug fixes in previous releases, refer to the release note(s) of interest from the SBC 5xx0-7000-SWe Documentation Home page.

The SBC Core supports Live Software Upgrade from releases listed in the table below:

Table 8: Supported Upgrade Paths

V06.xx	V07.xx	V08.xx	V09.xx
V06.00.00F009	V07.00.00R000	V08.00.00R000	V09.00.00R000
V06.00.00F014	V07.00.00F001	V08.01.00R000	V09.01.00R000
V06.02.00R000	V07.00.00F002	V08.01.00F001	V09.01.00R001
V06.02.00F000	V07.00.00F003	V08.01.00R001	V09.01.00R002
V06.02.01R000	V07.00.00F004	V08.01.00R002	V09.01.00R003
V06.02.01R001	V07.00.00F005	V08.01.00R003	V09.02.00R000
V06.02.01R002	V07.00.00F006	V08.01.00R004	V09.02.00R001
V06.02.01F001	V07.00.00S400	V08.01.00R005	V09.02.00R002
V06.02.01F002	V07.00.00S401	V08.01.00R006	V09.02.01R000
V06.02.01F003	V07.00.00S402	V08.01.00R007	V09.02.01R001
V06.02.01F004	V07.00.00S404	V08.01.00R008	V09.02.01R002
V06.02.01F005	V07.00.00S405	V08.02.00R000	V09.02.01R003
V06.02.01F006	V07.00.00S406	V08.02.00F001	V09.02.01R004
V06.02.01F007	V07.00.00S407	V08.02.00F002	V09.02.01R005
V06.02.01F008	V07.01.00R000	V08.02.00R001	V09.02.01R006
V06.02.01F009	V07.01.00R001	V08.02.00R002	V09.02.02R000
V06.02.01F010	V07.01.00R002	V08.02.01R000	V09.02.02R001
V06.02.01F011	V07.01.00R003	V08.02.01F001	V09.02.02R002
V06.02.01F012	V07.01.00R004	V08.02.01F002	V09.02.02R003
V06.02.02R000	V07.01.00F001	V08.02.01F003	V09.02.02R004
V06.02.02R001	V07.01.00F002	V08.02.02R000	V09.02.02R005
V06.02.02F001	V07.01.00F003	V08.02.02R001	V09.02.02R006
V06.02.02F002	V07.02.00R000	V08.02.02R002	V09.02.03R000
V06.02.02F003	V07.02.00R001	V08.02.02R003	V09.02.03R001
V06.02.02F004	V07.02.00R002	V08.02.02R004	
V06.02.02F005	V07.02.00S400	V08.02.02R005	
V06.02.02F006	V07.02.00S401	V08.02.03R000	
V06.02.02F007	V07.02.00S809	V08.02.03R001	

V06.02.02F008	V07.02.00S810	V08.02.03F001	
V06.02.02F009	V07.02.01R000	V08.02.04R000	
V06.02.02F010	V07.02.01R001	V08.02.04F001	
V06.02.02F011	V07.02.01R002	V08.02.04R001	
V06.02.02F012	V07.02.01R003	V08.02.04R002	
V06.02.02F013	V07.02.01R004	V08.02.04R003	
V06.02.02F014	V07.02.01F001	V08.02.04R004	
V06.02.03R000	V07.02.01F002	V08.02.05R000	
V06.02.03F001	V07.02.01F004	V08.02.05R001	
V06.02.03F002	V07.02.01F005	V08.02.05R002	
V06.02.03F003	V07.02.01S400	V08.02.05R003	
V06.02.03F004	V07.02.01R005	V08.02.05R004	
V06.02.03F005	V07.02.01R006		
V06.02.03F006	V07.02.01R007		
V06.02.03F007	V07.02.01R008		
V06.02.04R000	V07.02.01R009		
V06.02.04F001	V07.02.01R010		
V06.02.04F002	V07.02.02R000		
V06.02.05R000	V07.02.02R001		
	V07.02.02R002		
	V07.02.02R003		
	V07.02.02R004		
	V07.02.02R005		
	V07.02.02F001		
	V07.02.03R000		
	V07.02.03R001		
	V07.02.03R002		
	V07.02.03R003		
	V07.02.03R004		
	V07.02.03S400		
	V07.02.03S401		
	V07.02.04R000		
	V07.02.04R001		
	V07.02.04R002		
	V07.02.04R003		
	V07.02.04R004		
	V07.02.05R000		
	V07.02.05R001		
	V07.02.05R002		

	V07.02.05R003		
	V07.02.05R004		
	V07.02.05R005		
	V07.02.05R006		
	V07.02.05R007		
	V07.02.05R008		

Security Vulnerabilities

The following table displays the security vulnerabilities resolved in this release.

CVE	Risk	Description
CVE-2021-26691	Critical	In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
CVE-2018-20060	Critical	urllib3 before version 1.23 does not remove the Authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or scheme). This can allow for credentials in the Authorization header to be exposed to unintended hosts or transmitted in cleartext.
CVE-2021-31870	Critical	An issue was discovered in klibc before 2.0.9. Multiplication in the calloc() function may result in an integer overflow and a subsequent heap buffer overflow.
CVE-2019-18218	Critical	cdf_read_property_info in cdf.c in file through 5.37 does not restrict the number of CDF_VECTOR elements, which allows a heap-based buffer overflow (4-byte out-of-bounds write).
CVE-2021-31873	Critical	An issue was discovered in klibc before 2.0.9. Additions in the malloc() function may result in an integer overflow and a subsequent heap buffer overflow.
CVE-2021-31872	Critical	An issue was discovered in klibc before 2.0.9. Multiple possible integer overflows in the cpio command on 32-bit systems may result in a buffer overflow or other security impact.
CVE-2021-3246	High	A heap buffer overflow vulnerability in msadpcm_decode_block of libsndfile 1.0.30 allows attackers to execute arbitrary code via a crafted WAV file.
CVE-2020-35452	High	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
CVE-2021-29154	High	BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch displacements, allowing them to execute arbitrary code within the kernel context. This affects arch/x86/net/bpf_jit_comp.c and arch/x86/net/bpf_jit_comp32.c.
CVE-2020-35524	High	A heap-based buffer overflow flaw was found in libtiff in the handling of TIFF images in libtiff's TIFF2PDF tool. A specially crafted TIFF file can lead to arbitrary code execution. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2020-25672	High	A memory leak vulnerability was found in Linux kernel in llcp_sock_connect
CVE-2020-25671	High	A vulnerability was found in Linux Kernel, where a refcount leak in llcp_sock_connect() causing use-after-free which might lead to privilege escalations.
CVE-2021-33560	High	Libgcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to address a side-channel attack against mpi_powm, and the window size is not chosen appropriately. This, for example, affects use of ElGamal in OpenPGP.
CVE-2021-32399	High	net/bluetooth/hci_request.c in the Linux kernel through 5.12.2 has a race condition for removal of the HCI controller.
CVE-2021-26690	High	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
CVE-2021-3483	High	A flaw was found in the Nosy driver in the Linux kernel. This issue allows a device to be inserted twice into a doubly-linked list, leading to a use-after-free when one of these devices is removed. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. Versions before kernel 5.12-rc6 are affected

CVE-2021-28660	High	rtw_wx_set_scan in drivers/staging/rtl8188eu/os_dep/ioctl_linux.c in the Linux kernel through 5.11.6 allows writing beyond the end of the ->ssid[] array. NOTE: from the perspective of kernel.org releases, CVE IDs are not normally used for drivers/staging/* (unfinished work); however, system integrators may have situations in which a drivers/staging issue is relevant to their own customer base.
CVE-2021-2388	High	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).
CVE-2021-21702	High	In PHP versions 7.3.x below 7.3.27, 7.4.x below 7.4.15 and 8.0.x below 8.0.2, when using SOAP extension to connect to a SOAP server, a malicious SOAP server could return malformed XML data as a response that would cause PHP to access a null pointer and thus cause a crash.
CVE-2021-0512	High	In __hidinput_change_resolution_multipliers of hid-input.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-173843328References: Upstream kernel
CVE-2021-23133	High	A race condition in Linux kernel SCTP sockets (net/sctp/socket.c) before 5.12-rc8 can lead to kernel privilege escalation from the context of a network service or an unprivileged process. If sctp_destroy_sock is called without sock_net(sk)->sctp.addr_wq_lock then an element is removed from the auto_asconf_splist list without any proper locking. This can be exploited by an attacker with network service privileges to escalate to root or from the context of an unprivileged user directly if a BPF_CGROUP_INET_SOCK_CREATE is attached which denies creation of some SCTP socket.
CVE-2021-22555	High	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space
CVE-2021-31618	High	Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions and HTTP response is sent to the client with a status code indicating why the request was rejected. This rejection response was not fully initialised in the HTTP/2 protocol handler if the offending header was the very first one received or appeared in a a footer. This led to a NULL pointer dereference on initialised memory, crashing reliably the child process. Since such a triggering HTTP/2 request is easy to craft and submit, this can be exploited to DoS the server. This issue affected mod_http2 1.15.17 and Apache HTTP Server version 2.4.47 only. Apache HTTP Server 2.4.47 was never released.
CVE-2020-35523	High	An integer overflow flaw was found in libtiff that exists in the tif_getimage.c file. This flaw allows an attacker to inject and execute arbitrary code when a user opens a crafted TIFF file. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2021-33909	High	fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 does not properly restrict seq buffer allocations, leading to an integer overflow, an Out-of-bounds Write, and escalation to root by an unprivileged user, aka CID-8cae8cd89f05.
CVE-2021-23134	High	Use After Free vulnerability in nfc sockets in the Linux Kernel before 5.12.4 allows local attackers to elevate their privileges. In typical configurations, the issue can only be triggered by a privileged local user with the CAP_NET_RAW capability.
CVE-2021-31871	High	An issue was discovered in klibc before 2.0.9. An integer overflow in the cpio command may result in a NULL pointer dereference on 64-bit systems.
CVE-2021-33034	High	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.
CVE-2019-11324	High	The urllib3 library before 1.24.2 for Python mishandles certain cases where the desired set of CA certificates is different from the OS store of CA certificates, which results in SSL connections succeeding in situations where a verification failure is the correct outcome. This is related to use of the ssl_context, ca_certs, or ca_certs_dir argument.

CVE-2020-25670	High	A vulnerability was found in Linux Kernel where refcount leak in llcp_sock_bind() causing use-after-free which might lead to privilege escalations.
CVE-2021-30641	Medium	Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'
CVE-2020-1934	Medium	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
CVE-2021-0129	Medium	Improper access control in BlueZ may allow an authenticated user to potentially enable information disclosure via adjacent access.
CVE-2020-25673	Medium	A vulnerability was found in Linux kernel where non-blocking socket in llcp_sock_connect() leads to leak and eventually hanging-up the system.
CVE-2021-28964	Medium	A race condition was discovered in get_old_root in fs/btrfs/ctree.c in the Linux kernel through 5.11.8. It allows attackers to cause a denial of service (BUG) because of a lack of locking on an extent buffer before a cloning operation, aka CID-dbcc7d57bffc.
CVE-2021-3564	Medium	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.
CVE-2021-30002	Medium	An issue was discovered in the Linux kernel before 5.11.3 when a webcam device exists. video_usercopy in drivers/media/v4l2-core/v4l2-ioctl.c has a memory leak for large arguments, aka CID-fb18802a338b.
CVE-2019-11236	Medium	In the urllib3 library through 1.24.1 for Python, CRLF injection is possible if the attacker controls the request parameter.
CVE-2021-28971	Medium	In intel_pmu_drain_pebs_nhm in arch/x86/events/intel/ds.c in the Linux kernel through 5.11.8 on some Haswell CPUs, userspace applications (such as perf-fuzzer) can cause a system crash because the PEBS status in a PEBS record is mishandled, aka CID-d88d05a9e0b6.
CVE-2020-26558	Medium	Bluetooth LE and BR/EDR secure pairing in Bluetooth Core Specification 2.1 through 5.2 may permit a nearby man-in-the-middle attacker to identify the Passkey used during pairing (in the Passkey authentication procedure) by reflection of the public key and the authentication evidence of the initiating device, potentially permitting this attacker to complete authenticated pairing with the responding device using the correct Passkey for the pairing session. The attack methodology determines the Passkey value one bit at a time.
CVE-2021-29265	Medium	An issue was discovered in the Linux kernel before 5.11.7. usbip_sockfd_store in drivers/usb/usbip/stub_dev.c allows attackers to cause a denial of service (GPF) because the stub-up sequence has race conditions during an update of the local and shared status, aka CID-9380afd6df70.
CVE-2020-26147	Medium	An issue was discovered in the Linux kernel 5.8.9. The WEP, WPA, WPA2, and WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used.
CVE-2020-26139	Medium	An issue was discovered in the kernel in NetBSD 7.1. An Access Point (AP) forwards EAPOL frames to other clients even though the sender has not yet successfully authenticated to the AP. This might be abused in projected Wi-Fi networks to launch denial-of-service attacks against connected clients and makes it easier to exploit other vulnerabilities in connected clients.
CVE-2020-1927	Medium	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
CVE-2021-20292	Medium	There is a flaw reported in the Linux kernel in versions before 5.9 in drivers/gpu/drm/nouveau /nouveau_sgdma.c in nouveau_sgdma_create_ttm in Nouveau DRM subsystem. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker with a local account with a root privilege, can leverage this vulnerability to escalate privileges and execute code in the context of the kernel.

CVE-2021-2369	Medium	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Library). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2021-31829	Medium	kernel/bpf/verifier.c in the Linux kernel through 5.12.1 performs undesirable speculative loads, leading to disclosure of stack content via side-channel attacks, aka CID-801c6058d14a. The specific concern is not protecting the BPF stack area against speculative loads. Also, the BPF stack can contain uninitialized data that might represent sensitive information previously operated on by the kernel.
CVE-2021-34693	Medium	net/can/bcm.c in the Linux kernel through 5.12.10 allows local users to obtain sensitive information from kernel stack memory because parts of a data structure are uninitialized.
CVE-2020-26137	Medium	urllib3 before 1.25.9 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of putrequest(). NOTE: this is similar to CVE-2020-26116.
CVE-2020-36322	Medium	An issue was discovered in the FUSE filesystem implementation in the Linux kernel before 5.10.6, aka CID-5d069dbe8aaf. fuse_do_getattr() calls make_bad_inode() in inappropriate situations, causing a system crash. NOTE: the original fix for this vulnerability was incomplete, and its incompleteness is tracked as CVE-2021-28950.
CVE-2021-29155	Medium	An issue was discovered in the Linux kernel through 5.11.x. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory. Specifically, for sequences of pointer arithmetic operations, the pointer modification performed by the first operation is not correctly accounted for when restricting subsequent operations.
CVE-2021-38208	Medium	net/nfc/llcp_sock.c in the Linux kernel before 5.12.10 allows local unprivileged users to cause a denial of service (NULL pointer dereference and BUG) by making a getsockname call after a certain type of failure of a bind call.
CVE-2021-28688	Medium	The fix for XSA-365 includes initialization of pointers such that subsequent cleanup code wouldn't use uninitialized or stale values. This initialization went too far and may under certain conditions also overwrite pointers which are in need of cleaning up. The lack of cleanup would result in leaking persistent grants. The leak in turn would prevent fully cleaning up after a respective guest has died, leaving around zombie domains. All Linux versions having the fix for XSA-365 applied are vulnerable. XSA-365 was classified to affect versions back to at least 3.11.
CVE-2021-28950	Medium	An issue was discovered in fs/fuse/fuse_i.h in the Linux kernel before 5.11.8. A "stall on CPU" can occur because a retry loop continually finds the same bad inode, aka CID-775c5033a0d1.
CVE-2021-29650	Medium	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value, aka CID-175e476b8cdf.
CVE-2021-29647	Medium	An issue was discovered in the Linux kernel before 5.11.11. qrtr_recvmsg in net/qrtr/qrtr.c allows attackers to obtain sensitive information from kernel memory because of a partially uninitialized data structure, aka CID-50535249f624.
CVE-2020-7071	Medium	In PHP versions 7.3.x below 7.3.26, 7.4.x below 7.4.14 and 8.0.0, when validating URL with functions like filter_var($url, FILTER_VALIDATE_URL), PHP will accept an URL with invalid password as valid URL. This may lead to functions that rely on URL being valid to mis-parse the URL and produce wrong data as components of the URL.
CVE-2020-36311	Medium	An issue was discovered in the Linux kernel before 5.9. arch/x86/kvm/svm/sev.c allows attackers to cause a denial of service (soft lockup) by triggering destruction of a large SEV VM (which requires unregistering many encrypted regions), aka CID-7be74942f184.
CVE-2021-3573	Medium	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioct HCIUNBLOCKADDR or other way triggers race condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info(). A privileged local user could use this flaw to crash the system or escalate their privileges on the system. This flaw affects the Linux kernel versions prior to 5.13-rc5.

CVE-2021-31916	Medium	An out-of-bounds (OOB) memory write flaw was found in list_devices in drivers/md/dm-ioctl.c in the Multi-device driver module in the Linux kernel before 5.12. A bound check failure allows an attacker with special user (CAP_SYS_ADMIN) privilege to gain access to out-of-bounds memory leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to system availability.
CVE-2021-33910	Medium	basic/unit-name.c in systemd prior to 246.15, 247.8, 248.5, and 249.1 has a Memory Allocation with an Excessive Size Value (involving strdupa and alloca for a pathname controlled by a local attacker) that results in an operating system crash.
CVE-2020-24586	Low	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that received fragments be cleared from memory after (re)connecting to a network. Under the right circumstances, when another device sends fragmented frames encrypted using WEP, CCMP, or GCMP, this can be abused to inject arbitrary network packets and/or exfiltrate user data.
CVE-2021-38209	Low	net/netfilter/nf_conntrack_standalone.c in the Linux kernel before 5.12.2 allows observation of changes in any net namespace because these changes are leaked into all other net namespaces. This is related to the NF_SYSCTL_CT_MAX, NF_SYSCTL_CT_EXPECT_MAX, and NF_SYSCTL_CT_BUCKETS sysctls.
CVE-2020-24588	Low	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory as part of 802.11n), an adversary can abuse this to inject arbitrary network packets.
CVE-2020-29374	Low	An issue was discovered in the Linux kernel before 5.7.3, related to mm/gup.c and mm/huge_memory.c. The get_user_pages (aka gup) implementation, when used for a copy-on-write page, does not properly consider the semantics of read operations and therefore can grant unintended write access, aka CID-17839856fd58.
CVE-2021-22898	Low	curl 7.7 through 7.76.1 suffers from an information disclosure when the `-t` command line option, known as `CURLOPT_TELNETOPTIONS` in libcurl, is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending NEW_ENV variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal information to the server using a clear-text network protocol.
CVE-2021-21781	Low	An information disclosure vulnerability exists in the ARM SIGPAGE functionality of Linux Kernel v5.4.66 and v5.4.54. The latest version (5.11-rc4) seems to still be vulnerable. A userland application can read the contents of the sigpage, which can leak kernel memory contents. An attacker can read a process's memory at a specific offset to trigger this vulnerability. This was fixed in kernel releases: 4.14.222 4.19.177 5.4.99 5.10.17 5.11
CVE-2021-2341	Low	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2021-22924	Low	libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse, if one of them matches the setup.Due to errors in the logic, the config matching function did not take 'issuercert' into account and it compared the involved paths *case insensitively*,which could lead to libcurl reusing wrong connections.File paths are, or can be, case sensitive on many systems but not all, and caneven vary depending on used file systems.The comparison also didn't include the 'issuer cert' which a transfer can setto qualify how to verify the server certificate.
CVE-2020-24587	Low	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to decrypt selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed.

Resolved Issues

Resolved Issues in 09.02.03R002 Release

The following Severity 1 issues are resolved in this release:

Table 9: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-113305 | SBX-114425	1	PortFix SBX-113305: DNS recovery packet count of DSCP as "0". **Impact:** The DNS probe packets are sent from the SBC with a DSCP value of "0". **Root Cause:** The configured DSCP values were not set for DNS probe keepalive packets. **Steps to Replicate:** 1. Configure DNS server with a DSCP value. 2. Ensure the DNS server blacklisting is enabled. 3. Ensure the DNS query is configured DNS server. 4. Shut down the DNS server during this process. Result: Observe that the configured DNS server is blacklisted and sending DNS probe packet towards a DNS server with configured DSCP value.	The code is modified to set a configured DSCP value for packets, including DNS probe packets. **Workaround**: None.
SBX-114012 | SBX-114320	1	PortFix SBX-114012: The SMM is not working when the From contains an escape character. **Impact:** The SMM may fail to parse a display name in double quote string when the string has more than one escape characters next to each other of a header. **Root Cause:** Logical error in parsing logic that causes a parsing failure. **Steps to Replicate:** Configure a rule to access double quote string display name of uri header, or any parameter. Ensure there is an input display name, such as From: "PhoneLite \\\"test1\\\"test2 " <sip:[field0]@dns.com>;tag=testing	The code is modified to address the issue. **Workaround**: None.
SBX-109056 | SBX-114568	1	PortFix SBX-109056: The SBC 5400 MS Teams CQ has transfers issues. **Impact:** When a call with DLRBT enabled undergoes more than one transfer with REFER signaling and the final transferee does not accept the call, the SBC does not correctly reconnect the call back to the transferor. **Root Cause:** For an A-to-B call, if B, for example, successfully REFERS the call to C, and then C attempts to REFER the call to D (or back to B), the SBC plays a ringtone towards A while the REFER is taking place. However, when D rejects the call with a 480 "Temporarily not available" message, the SBC does not correctly disable the call context that is playing the tone, nor does it correctly re-enable the A-to-C call association. **Steps to Replicate:** 1. With DLRBT configured on ingress and egress of SBC. Establish an A-to-B call through the SBC. 2. Send a REFER from B to refer the call to C and complete the refer related signaling. This results in an A-to-C call. 3. Send a REFER from C to refer the call to D. Do not answer the call at D but reject it with a 480 "Temporarily not available" message. 4. Verify that the SBC stops playing tone towards A and re-establishes the A-to-C call again and media can correctly flow between A and C.	The code is modified to disable the tone playing towards A when a 480 is received and then correctly re-enable the call association back to the transferor. **Workaround**: None.
SBX-114315 | SBX-114427	1	PortFix SBX-114315: An SBC failover occurred because of an SCM Process core. **Impact:** An SCM core can occur if the hostName in the From Header is longer than 64 bytes. **Root Cause:** The code is copying the host name into an array that is not long enough to hold it. This results in memory corruption. **Steps to Replicate:** Make a call where the hostName in the From Header is longer than 64 bytes.	The code is modified to use the correct size when copying the host name. **Workaround**: None.

The following Severity 2 issue is resolved in this release:

Table 10: Severity 2 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-112547 | SBX-114405	2	PortFix SBX-112547: The SBC routes call to 2nd DNS record if 503 is received after 18x. **Impact:** The SBC routes an INVITE to next DNS record if 503 is received after 18x. Also, even when the dnsCrankback flag is disabled, on getting 503/INVITE timeout case, the SBC reroutes an INVITE to next DNS record. **Root Cause:** Due to a design defect, the SBC tries the next DNS record even if an error response is received after an 18x. Also, retrying the next DNS record during a 503/timeout when dnsCrankback flag is disabled is legacy behavior. This behaviour is changed to retry the next DNS record only when the dnsCrankback flag is enabled. **Steps to Replicate:** 1. Configure the DNS server with two routes for the FQDN route. 2. Make an A-to-B call. 3. The SBC sends an INVITE to first DNS record of and B sends 18x and the 503.	The code is modified to not apply the DNS crankback procedure if an error response is received after a 18x. Additionally, the default behavior of handling timeout/503 when the dnsCrankback is disabled is updated as part of this fix. With this fix, the SBC retries for the next DNS record only when dnsCrankback is enabled to ensure the error responses match the reasons configured in the crankback profile. **Workaround**: None.
SBX-113053 | SBX-114355	2	PortFix SBX-113053: Race Condition when 183 and 200 OK (INVITE) are received simultaneously. 200 OK is not relayed to other side. **Impact:** Race condition between internal processing of the 200 OK for an UPDATE and a received 183 Session Progress. **Root Cause:** After a 200 OK (UPDATE) is received, followed immediately by receipt of 183 Session progress, a subsequent 200 OK (INVITE) containing P-Early-Media header is queued indefinitely at egress when downstreamForking is enabled and earlyMedia forkingBehaviour is pemPriority. **Steps to Replicate:** Egress SIP trunk group has downstreamForking is enabled and earlyMedia forkingBehaviour is pemPriority. Make a call so that egress signaling is as follows: --> INVITE (with SDP and P-Early-Media: supported) <-- 100 Trying <-- 183 Session Progress (with SDP and no P-Early-Media) --> PRACK <-- 200 OK (for PRACK) --> UPDATE (with SDP) <-- 200 OK (for UPDATE with SDP) <-- 183 Session Progress (no SDP but P-Early-Media: sendrecv) --> PRACK <-- 200 OK (for PRACK) <-- 200 OK (for INVITE) (This message gets queued forever).	The code is modified to eliminate the race condition. **Workaround**: None.
SBX-113614 | SBX-114546	3	PortFix SBX-113614: The ActiveRegCount is greater on the INGRESS side. **Impact:** When registration(s) take longer than 90 seconds to complete, the ingress zone's activeRegs count can increment, but not decrement, when the registration terminates. This may cause the ingress zone's activeRegs count to grow incorrectly, and never reach ZERO (even after all registrations are terminated). **Root Cause:** The SIPFE and SIPSG RCB allocation/deallocation become out of sync, indirectly causing the ingress zone's activeRegs count to increment and not decrement. **Steps to Replicate:** Perform the endless REGISTER/403, or REGISTER/503, or REGISTER/603 sequence.	The code is modified to handle registration(s) that take longer then 90 seconds to complete. In this case, the SIPFE restarts the registration bind timer and avoids "prematurely" deallocating the RCB so that the FE and SG RCB(s) stay "in-sync". **Workaround:** None.
GSX-54479 | SBX-114528	4	PortFix GSX-54479: The isup-oli parameter is sending a single digit OLI value in isup-oli parameter for values 0-9. **Impact:** The SBC sends all OLI digits as a single digit. **Root Cause:** This functionality is not within spec. **Steps to Replicate:** Make a call that uses OLI parameter.	The code is modified to add a leading 0 for OLI digits 0-9. **Workaround**: None.

Resolved Issues in 09.02.03R001 Release

The following Severity 1 issues are resolved in this release:

Table 11: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-113954 | SBX-104348	1	PortFix SBX-104348: STUN was received on the SBC and the SBC considers these packets are arriving on another IP. And as a result, the STUN wasn't processed. **Impact:** The SBC passes the STUN packets to wrong IP address when it received them on the alternate IP. **Root Cause:** The SBC always uses the primary IP address of LIF to send out the packet, even when it receives the STUN packets on the alternate LIF IP. **Steps to Replicate:** STUN received on alternate IP of LIF and the SBC does not respond correctly, which appears as the SBC not processing it.	The code is modified so the XRM traverses the IP address list to match the address where it received the packet, instead of directly using the primary IP to send the packets. **Workaround**: None.
SBX-114073 | SBX-113853	1	PortFix SBX-113853: The SBC experienced an intermittent crash. **Impact:** When multiple duplicate Diversion headers are received and stiProfile is enabled and configured on the ingress trunk group, the SBC dumps core. The issue only occurs if six or more Diversion headers are received but fewer than five of them are unique. **Root Cause:** Removing duplicated Diversion headers from information sent to the PSX causes crash. **Steps to Replicate:** 1. Configure the stiProfile, enable, and assign to ingress trunk group. 2. Send an SIP INVITE containing six Diversion headers but only two of them are unique. In other words, send in two Diversion headers repeated three times.	The code is modified to remove the duplicate Diversion headers from information sent to the PSX. **Workaround**: None.

The following Severity 2 issue is resolved in this release:

Table 12: Severity 2 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-114019	2	The DBG logs was rolling rapidly with UacSendUpdate messages. **Impact:** The SBC DBG logs were filling up quickly with the following log message. 114 10192021 114119.823662:1.01.03.16703.MAJOR .SIPSG: UacSendUpdate - local answer for UPDATE: LegSide=Ingress **Root Cause:** The code was mistakenly printing logs at the MAJOR level. **Steps to Replicate:** The log is generated during a call where the SBC tries to send an UPDATE out to ingress leg while the PRACK is pending for previous 18x sent. The following control also needs to be disabled on the trunk group the messages are being sent on. set addressContext default zone <zone name> sipTrunkGroup <TG name> signaling doNotAutoAnswer <enable/disable>.	The code is modified to only print the logs at an INFO level. **Workaround**: None.

Resolved Issues in 09.02.03R000 Release

The following Severity 1 issues are resolved in this release:

Table 13: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution

SBX-112996 | SBX-113115	1	PortFix SBX-112996: There was a SCM core dump. **Impact:** A rare race condition triggers a bug that caused SCM to core. **Root Cause:** A bug in the code causes an attempt to access freed memory. This Gateway-to-Gateway bug has has existed for a very long time, but was not encountered until now. The bug is triggered by a rare race condition. **Steps to Replicate:** This bug was found through code inspection. The bug is triggered by a rare race condition that is not reproducible.	The code is modified to avoid accessing freed memory. **Workaround:** There is no workaround.
SBX-112366 | SBX-112738	1	PortFix SBX-112366: A customer's redundancy had an unexpected switchover. **Impact:** The SBC is coring in the IPsec/IKE code when a call is using an IKE Protection Profile that was configured without any algorithms. **Root Cause:** The SBC coredumped in the IPsec/IKE code due to an attempt to de-reference a NULL pointer. The pointer is NULL because the IKE Protection Profile being used was configured without any algorithms. **Steps to Replicate:** 1. Configure an IKE Protection Profile without any algorithms. 2. Run a call that will use this profile.	The code is modified to check for a NULL pointer and take the correct error path when the pointer is NULL. **Workaround:** When configuring the IKE Protection Profiles, ensure that an algorithm is configured for this profile.
SBX-112349 | SBX-112847	1	PortFix SBX-112349: The SBC releases a 132 Release code (MODULE FAILURE) message when running an audit call. **Impact:** An Async CMD Error reported by XRM that triggered call being torn down with release code 132 when running a call audit. **Root Cause:** Ribbon lacks the necessary level of detail to conclusively determine the root cause. **Steps to Replicate:** Since we do not know the exact condition and what types of resources were involved, we cannot provide detailed test steps for this case. Suggest running regular regression tests to attempt to reproduce the issue.	The code is modified for LE2MCAST, LE2MCAST_RTCP, LE2SPLITTER. The changes provided are based on source code inspection. **Workaround:** N/A
SBX-112677 | SBX-112715	1	PortFix SBX-112677: The SCMP cored in Late media passthrough calls over a GW-GW. **Impact:** There was a coredump for a late media passthrough case. **Root Cause:** Dereferences a NULL Pointer. **Steps to Replicate:** For the SBC GW-GW setup. Enable the LM passthrough flag. Run the following procedure: 1. Ingress sends LM Invite. 2. Egress sends 18x with SDP. 3. Ingress sends SDP in Prack. 4. Once call is established, send LM re-Invite request from Egress. 5. Ingress responds with 200 Ok and receives ACK with SDP. 6. Ingress sends LM re-Invite request towards egress.	The code is modified to stop the coredump. **Workaround:** None.
SBX-107747 | SBX-112649	1	PortFix SBX-107747: Cyclic switchover tests - Observed a PRS Process core dump on the M-SBC1. **Impact:** If an M-SBC instance transitions to active shortly after the instance comes up as standby, when certain performance stats are collected, the PRS process will crash. **Root Cause:** When the instance comes up as a standby, the active instances send their metavariable information to the new standby instance. This information is sent twice for each active instances. The first metavariable information for each active instance is not received by the PRS process because the PRS process is not ready to receive it. If the instance switches to active before the second set of metavariable information is received, then the new active will not have metavariable information from the former active, which causes the PRS crash. **Steps to Replicate:** 1. Bring up an MSBC 4-1 cluster. 2. Restart the standby instance. 3. Immediately after the standby instance is fully up, restart one of the active instances. 4. After the standby instance is fully up as the active instance, in the CLI run the following command: unhide debug show table global icmpGeneralGroupCurrentStatistics	The code is modified so the CHM process queues the first set of metavariable information until the PRS process is ready to receive it, and then sends the information to the PRS process. **Workaround:** None.

SBX-112445 | SBX-112880	1	PortFix SBX-112445: Conference calls fail when taking a recorded (SIPREC) path, but they work when SIPREC settings are not enabled. **Impact:** The SBC cleanup call during hold retrieval for the transferred call. This issue is observed only when the SIP Rec is enabled. **Root Cause:** Invalid operation on media resource during call hold/unhold for the transferred call leads call to cleanup. This issue is observed only when the SIP Rec is enabled. **Steps to Replicate:** 1. Enable the SIP Rec. 2. Make a blind/attended call transfer and after successful transfer, perform a call hold and unhold.	The code is modified to not perform any invalid operation on media resources during call hold/unhold for the transferred call. **Workaround:** NA.
SBX-112561 | SBX-112836	1	PortFix SBX-112561: Regexp string was not exported by “user-config-export” **Impact:** In the Regex, the SMM is lost while exporting a configuration using the user-config-export CLI command. **Root Cause:** The XML formatting is trimming empty node values. **Steps to Replicate:** 1. Create the SMM Profile using the following command strings: set profiles signaling sipAdaptorProfile ESMM state disabled set profiles signaling sipAdaptorProfile ESMM advancedSMM disabled set profiles signaling sipAdaptorProfile ESMM profileType messageManipulation set profiles signaling sipAdaptorProfile ESMM rule 1 applyMatchHeader one set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 1 type message set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 1 message set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 1 message messageTypes requestAll set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 type header set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header name WWW-Authenticate set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header condition exist set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header numberOfInstances number 1 set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header numberOfInstances qualifier equal set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 type parameter set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 parameter set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 parameter condition exist set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 parameter paramType generic set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 parameter name realm set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 type header set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 operation regsub set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 headerInfo headerValue set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 from set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 from type value set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 from value 172.xx.xx.xxx set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 to set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 to type header set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 to value WWW-Authenticate set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 regexp set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 regexp string " " set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 regexp matchInstance all commit 2. Run the following CLI command to export the configuration: user-config-export test.xml /profiles/signaling/sipAdaptorProfile 3. Delete the exported profile from the CLI with the following command: delete profiles signaling sipAdaptorProfile ESMM commit user-config-import test.xml 4. Run the following command: show configuration profiles signaling sipAdaptorProfile | display set | match string 5. Check if the Regex string field, and restore the original value.	The code is modified to use the external tool "xmllint" to format the XML. **Workaround:** Manually edit the field in the XML file after an export and before an import to correct the issue.

SBX-111126 | SBX-112531	1	PortFix SBX-111126: In the case of delayed offer, the SBC changes the attribute “a=sendonly” into “a=recvonly” before relaying the 200 OK INVITE. **Impact:** The direction attribute in 200OK sent in response to late media reinvite is set to an incorrect value when the direction attribute received in 200OK from other side is a value other than a=sendrecv. **Root Cause:** The datapathmode on the side receiving the late media invite is incorrectly copied from the SBC local datapathmode from the answer leg PSP receiving 200OK when sendSbcSupportedCodecsInLateMediaReinvite flag is enabled. **Steps to Replicate:** 1. Enable the sendSbcSupportedCodecsInLateMediaReinvite on the TG towards UAC. 2. Send a direction attribute a=sendonly/recvonly/inactive from the UAS. 3. Send the 200OK to UAC should have direction attribute as expected (a=sendonly/recvonly/inactive respectively) and media is as per expectation. UAC----------SBC----------UAS INV(no sdp)->\ INV(a=sendrecv)->\ <-200OK(a=sendonly/recvonly/inactive)\ <-200OK(a=sendonly/recvonly/inactive)\ ACK(sdp)->\ ACK(no sdp)->	The code is modified so the datapathmode in the active PSP on late media offer side is recomputed when the sendSbcSupportedCodecsInLateMediaReinvite flag is enabled. **Workaround:** Disable the sendSbcSupportedCodecsInLateMediaReinvite IPSP flag on TG receiving late media reinvite.
SBX-112624	1	The SBC is unable to recognize a PRACK message, when call hunts to a secondary route. **Impact:** The PRACK was rejected with a 481 when the end-to-end PRACK is active if a call is cranked-back following a successful end-to-end PRACK on the earlier route. **Root Cause:** If end-to-end PRACK is performed on the first route and then a late crank-back occurs, subsequent PRACK is rejected because stale information is present from the first route. **Steps to Replicate:** 1. Ensure the end-to-end PRACK is supported. 2. Make a SIP-SIP call that routes and 18x is received on the first route. As a result, the PRACK procedure is successful. 3. Have the call fail on the first route, e.g. with 404, and the SBC configured to crank-back to a second route. The 18x is received on the second route. When the calling party responds with PRACK, the call has a 481 in response.	The code is modified so that end-to-end PRACK information is started fresh for each route. **Workaround:** None.
SBX-112307	1	A customer's SBC 7000 SIPREC metadata did not contain an ‘AOR’ parameter value. **Impact:** In the SIPREC, the metadata sender and receiver's AOR fields for the tel URI were not populated properly. **Root Cause:** Due to defect in the design, these fields were populated incorrectly. **Steps to Replicate:** 1. Configure the SBC with SIP Rec server. 2. Run a basic call with "tel" URI in From and To header.	The code is modified to populate as per requirements/standard. **Workaround:** Not Applicable.
SBX-106316	1	The call established prior to a switchover fails when put on hold after a switchover. **Impact:** The call established prior to a switchover with a dynamic payload type fails when put on hold after switchover. **Root Cause:** After a switchover, while processing the hold request, it was unable to locate the codec due to an issue in reconstruction of some flags in PSP data. **Steps to Replicate:** 1. Have a HA setup. 2. In IPSP, enable "Minimize relay of media changes from other call leg" flag and "lockdown preferred codec" is enabled. 3. Establish a call with dynamic codec like AMR. 4. Perform a switchover, once standby becomes active send a call hold request. 5. After a short period of time, send an call-un-hold request. result: Call hold invite should be successful with 200 ok for that and call un-hold should also be successful.	The code is modified so that necessary flag for dynamic payloads in PSP data are reconstructed properly. **Workaround:** Disable“Lock Down Preferred Codec” and enable “Relay Data Path Mode Changes".

SBX-111498	1	The SBC Ladder diagram (.TRC file) shows a response from the wrong IP for a 400 Bad Request. **Impact:** When an INVITE (with malformed syntax) is sent to a leg1 (pkt1) SIP signaling IP for the SBC, the SBC responds with a 400 Bad request. In the TRC log, for a 400 Bad request PDU, the Local IP/port is printed with a leg 0 (pkt0) SIP Signaling IP Address instead of leg 1 SIP Signaling IP Address. This occurs only when the SBC sends error response message. **Root Cause:** During formatting of Error message, the code is incorrectly using the pkt0 SIP Signaling IP Address instead of a pkt1 SIP Signaling IP Address resulting in the incorrect value being printed in the TRC log. **Steps to Replicate:** 1. Set up a SIP-SBC-SIP. 2. Enable trace logging with level4 and key "peerIpAddress" 3. Run a SIP-SIP call, send INVITE with malformed syntax to pkt1 SIP signaling IP address such that the SBC sends a 400 Bad Request. 4. Verify that in the TRC log, for 400 Bad request PDU, the local IP value is pkt 1 SIP signaling IP address, same source IP where the INVITE message lands.	The code is modified to correctly read the SIP Signaling IP Address of the leg where the call lands. **Workaround:** None.
SBX-106037	1	The SBC 7000 is sending a re-INVITE before receiving an ACK to the 200 OK - multi-stream call. **Impact:** The SBC removes transcodable codecs when the application media m-line is present with port as 0. This results in the SBC sending a re-INVITE without SDP. **Root Cause:** By default, the SBC does not support transcoding on multi-stream calls. The problem here was that the code incorrectly identified that there was an application stream present even when the port was set to 0. This made it appear as a multi-stream call and resulted in the transcodable codecs being removed. **Steps to Replicate:** Test Case 1: GW-GW Scenario 1. Make a G711-G711 GW-GW call. The SBC will send BYE to peers. The call will fail. Test Case 2: Non GW-GW Scenario 2. Configure below PSPs on ingress and Egress legs Ingress PSP: G729, G711U, G711A This Leg – G711U, G711A, EFR, EVRC, Other Leg – G711U, G711A, Enable Transcode if different pktsize, dtmf, silence suppression and honor preference. Egress PSP: G711SS This Leg – G711U, G711A, Other Leg – G711U, G711A, Enable Transcode if different pktsize, silence suppression 3. Make a G711-G711 call. The user observes logs in TRC file and the SBC will send BYE to peers. The call will fail.	The code is modified so that the stream with a port 0 is effectively ignored when processing transcodable codecs. **Workaround:** Enabling "AllowAudioTranscodeForMultiStreamCalls" flag on both ingress and egress PSPs will solve the issue.
SBX-112557	1	The password policy is not recognized by the SBC. **Impact:** The password policy not recognized by the SBC. By default, the admin rules were taken. **Root Cause:** Password policy was assigned based on roles of the user. **Steps to Replicate:** Go to Administration/Application Management. In Configure Password Rules tab, check by enable or disable "Use Separate Password Rules for Administrators" where you are able to change the password policy or not in change password model.	The code is modified to use the state variable in PasswordRule class **Workaround:** Add new variable named "state" to PasswordRule Class as a workaround.
SBX-111743	1	The SBC block list IP with the wrong port. **Impact:** The ARS block lists port 0, when an INVITE contains a Route header without a port number, and 503 response contains a Retry-After header. **Root Cause:** The code did not support a case where no port number is provided. **Steps to Replicate:** 1. Configure ARS Retry-After profile. 2. Enable callRouting useRouteSet received in ingress and egress trunk groups. 3. Use the UAC to send an INVITE containing Route without port number: Route: <sip:172.xx.xxx.xx;lr;dtg=SBX_EXAMPLE> The UAS responds with 503 Service Unavailable with Retry-After header use CLI to check egress zone sipArsStatus.	The code is modified so when no port number is set, we now retrieve the port number from the transaction control block. **Workaround:** Define an SMM rule that adds the port number (5060) if the Route header in the initial INVITE does not contain a port number.
SBX-113471	1	Multiple SBC core dumps were detected. **Impact:** There was forking hashtable corrupted memory. **Root Cause:** Possibility of forking control fails to remove from hashtable when the resource is cleaned up. **Steps to Replicate:** Unable to reproduce. Run high load with a NAPT, upstream forking and registration and taking a SIP signaling port down/up.	The code is modified to ensure the forking call is removed from hashtable when free. **Workaround:** None.

SBX-112322	1	The SBC cored when the subscribe crankback failure. **Impact:** When a relay Subscribe tried to crank back for the second route and if the SBC does not find trunk group, the SBC may core. **Root Cause:** The SBC cores due to duplicated memory freed. **Steps to Replicate:** Configure two routes for the relay Subscribe. The second route is invalid. After the first route exhausted, the SBC try to cranked back for the second route. The SBC fails to find trunk group for the second route.	The code is modified to prevent duplicated memory to be freed. **Workaround:** Correct the second route.
SBX-113183 | SBX-107753	1	PortFix SBX-107753: After the LSWU, the apache2 not coming up, resulting in an EMA or PM access issue. **Impact:** After an upgrade, the Apache did not start. **Root Cause:** Apache did not start due to a timeout while requesting a password. The Apache would need to be restarted manually especially in case of a failed upgrade. **Steps to Replicate:** 1. Perform an upgrade (LSWU/standalone). 2. If upgrade has failed, verify that the apache has come up properly with default keys and cert. 3. If upgrade has succeeded, verify that first Apache came up properly with default keys, then after app start, the installed keys and certs are being used by the Apache.	The code is modified to find any occurrence of the one-time-issue of server key getting corrupted in the future. **Workaround**: In case of a failed upgrade or apache startup failure restart apache or apply the workaround mentioned in an issue relating to the apache2 failing after an LSWU.
SBX-113426 | SBX-112447	1	PortFix SBX-112447: The SIPRec recording failed for an EGRESS call with GCID 291515755. **Impact:** The SIPREC sessions fail with the following "MAJOR" logs when a CS call is going for call a modification with re-INVITE and a corresponding re-INIVTE is triggered for this towards the SRS while a previous SRS SIP transaction is pending. 159 08192021 154751.374314:1.02.00.26912.MAJOR .SIPSG: sipsgRec.c (-5062) 529606794. [SipSgSendSRSMetadataUpdateCmd] SipSgSendSdpCmd Failed with status 491 185 08192021 154751.375973:1.02.00.26913.Minor .SIPSG: SIPRec Recording failed for EGRESS call with GCID 291518377 for Recorder 10.xx.xxx.xx:xxxx. Trunkgroup of Recorder: NICE_PRI_TG **Root Cause:** The SBC always attempted to send another offer towards SRS even when a offer-answer was pending and this resulted in SRS session failure. **Steps to Replicate:** Use the following set up to reproduce the issue. 1. Main Call (CS) session established. 2. SIPREC session (RS) is established. 3. CS call goes for modification with re-INVITE (Hold/Codec change). A SIPREC re-INVITE is triggered (based on CS re-INVITE). 4. The SRS does not respond for SIPREC re-INVITE. 5. Before the SRS answers the re-INVITE, a CS call triggers yet another modification with re-INVITE (unhold/codec change). 6. The SBC attempts to trigger SIPREC RE-INVITE again even when the previous transaction is pending and results in SRS session failure.	When a SIP Offer-Answer towards SRS is in progress, SBC shall not attempt to send another offer and instead shall queue the latest event until the current offer-answer is complete. **Workaround**: None.
SBX-113196	1	A SCM Process coreump occurred on the SIGABRT. **Impact:** When the INVITE message contains trunk group/trunk context parameter information and the context is an FQDN, then the SBC can use this information to formulate the IP Peer information if there is none supplied from the PSX. This can result in an SCM process coredump, if multiple routes are returned from the PSX. **Root Cause:** The internal processing code did not account for multiple routes and it was always freeing memory that was possibly assigned to the first route. However, when processing the second or subsequent routes in a crankback scenario, the memory on the first route freed once when routing the call on the second route and then again when the call was actually released. This second freed memory was invalid and results in a coredump. **Steps to Replicate:** 1. Pass in the trunk group and trunk context parameters that use FQDN information. 2. Ensure the PSX returns 3 routes and no IP Peer IP or FQDN information. 3. Return a crankback status code in response to the INVITEs sent on route 1 and route 2. 4. Release the call.	The code is modified to correctly manage the memory on the route being used for the call. The code change frees and allocates memory consistently for a route to avoid freeing the memory twice. **Workaround**: Remove the trunk group/context using the SMM from the received INVITE. Ensure the PSX only returns one route when processing trunk group /context information.

The following Severity 2-4 issues are resolved in this release:

Table 14: Severity 2-4 Resolved Issues

Issue ID	Sev	Problem Description	Resolution

SBX-112857 | SBX-113197	3	PortFix SBX-112857: Increase the VNFM response timeout. **Impact:** By default, the VNFR logic had a 5 second timeout to get responses from VNFM for the REST requests that it sent, but it has been observed that in certain networks this timeout value is not enough. This leads to the VNFR timing out while the VNFM was still trying to send back a response and the VNFR never reported ready state in the VNFM. **Root Cause:** A delay of 5 seconds was originally thought to be long enough but across multiple networks, this was insufficient. **Steps to Replicate:** Try a relocation operation with VNFM across multiple sites and ensure the VNFR status returns to ready.	The code is modified so the timeout is now increased to 20 seconds. **Workaround:** None.
SBX-112487 | SBX-113200	2	PortFix SBX-112487: The LI connection to media server was not connected on a switchover. **Impact:** When using a PCSILI (P-com-session-info flavour of LI) in an N:1 M-SBC setup and running the SBC release 8.2 or later, if there is a switchover, the connection to the LI server might not be re-established. **Root Cause:** The standby instance was trying to maintain information about the operational status of the interface used for LI processing. But this was only happening correctly for the first instance. The status of the other instances was being misinterpreted and lost. So during the transition to active the LI code thought the interface was not available and did not try to establish the connection to the LI server. **Steps to Replicate:** In an N:1 setup perform switchovers from each active instance to the standby and check that the connection to the LI server is restored.	The code is modified to collect the status of the interface after the instance is transitioned from standby to active, so that accurate interface information is available for LI processing. **Workaround:** Bouncing the interface (e.g. ifup/ifdown that is used for LI connection), will help to recover the connection.
SBX-109006 | SBX-110819	2	PortFix SBX-109006: The DSP DHC had a Failure and failed to coredump. **Impact:** The FPGA based DSP Health Check (DHC) fails and as a result, no DSP coredump is collected. **Root Cause:** The root cause for DHC failure is not known. However, subsequent coredumps failed due to a lack of reception of the DSP BOOTP packets, which is a hard failure. It is speculated that both issues are related. **Steps to Replicate:** Instrument the code to replicate the issue.	Reboot the node instead of running an application restart to address the issue. **Note:** This is not a fix for the original issue, but just a proposed workaround to prevent or reduce further failures. **Workaround:** None.
SBX-112971 | SBX-113352	2	PortFix SBX-112971: The diameter process cored continuously when creating the diamNode entry. **Impact:** The diameter process acts as a client and server. When it acts as server, on accepting TCP connection from the remote diameter client, the diameter process crashes due to an invalid operation. **Note**: There is no use case where the diam process accept connection from remote diameter client, so this scenario not covered in our earlier testing. This issue observed during misconfiguration. **Root Cause:** On accepting TCP connection from the remote diameter client, the diameter process tries to perform an invalid operation (null pointer access) and due to this, the diameter process crashes. **Steps to Replicate:** Configure the diameter node in the SBC and simulate TCP client application that connects the diameter server (on port 3868).	The code is modified so the diameter process does not perform any invalid operation. **Workaround:** Do not configure same IP address for the peer and for diameter node.
SBX-113413 | SBX-113535	2	PortFix SBX-113413: The call failure with an extra INVITE is sending. **Impact:** If A calls B over the SBC, the SBC sends INV with sendrecv to B. B sends 180/200 with recvonly. After call is established, the SBC sends a re-INVITE to B with data path mode as sendonly. **Root Cause:** As part of a previous issue, a behavior change was introduced so that the SBC sends a hold re-INVITE (received from the network) to the other end. This was only for the cases where call is already on hold but data path mode is changed. **Steps to Replicate:** 1. Send an INVITE from A to B. The SBC sends sendrev to egress. 2. From B, send a 180 with recvonly. 3. From B, send a 200 Ok with recvonly. A to B is connected. When call is connected, there should not be an re-INV towards egress leg (with recvonly).	The code is modified so in the case when the SBC receives a re-INVITE from network and data path mode is changed, it triggers a new re-INVITE to the other leg. In other cases, it would be same behavior (prior to SBX-111611). **Workaround:** None.

SBX-107396 | SBX-112247	2	PortFix SBX-107396: Error "SYS ERR - Error 0x3b Line 666" was being printed frequently. **Impact:** SYS ERR repeatedly logged in SYS logs. **Root Cause:** The SYS ERR seems to only occur for audio encoding type 0x3b, which is SPEEX_8. But we don't have enough information to determine the call flow that triggered it. **Steps to Replicate:** The steps cannot be reproduced.	The code is modified to replace the SYS ERR with a major level debug message with the GCID and audio encoding type to help future debugging. **Workaround:** None.
SBX-110592 | SBX-112526	3	PortFix SBX-110592: There was a misleading TRC message when issuing the callTrace action command start command. **Impact:** The misleading TRC message when issuing a "callTrace action command start command". **Root Cause:** There was no alarm/log message indicating a global call trace start action command. **Steps to Replicate:** Issue the callTrace action command and observe the Trace log. admin@vsbxsus2> request global callTrace action command start Sonus Networks, Inc.00000000016000000000000000000000128V08.02.06A002 00000000000000000000000000000TRC20210820145937000000000000000 072 08202021 145941.298910:1.01.00.00002.Info .NRM: Call Trace Reset	The code is modified to display correct message indicating call trace being reset. **Workaround:** None.
SBX-110755 | SBX-112791	2	Portfix SBX-110755: The ACL rules configured with ipInterface are disabled on every SBC start/restart in SBC5400/10GB pkt configuration. **Impact:** The IPACL rules created with ipInterface defined are not getting installed on the SBC 5400 systems when there is no license present, or after a license is added. **Root Cause:** The NP will not install an IPACL rule with an ipInterface defined if that interface is not UP and active. The SBC will retry to install failed rules when it sees the port come up. In this scenario the timing is off, however, it tries too soon as the physical port is up but the associated ipInterface is not yet up. **Steps to Replicate:** The test involves a SBC 5400 without a license for its 10G packet port. The IPACL rules with ipInterface defined on that packet port will then fail to install. Once the license is successfully added, the IPACL rules should be installed.	The code is modified to add an additional delay before attempting to reinstall the failed IPACL rules when the port comes up and to look for an additional failure that starts a timer and try again. **Workaround:** Do not use IPACL rules with ipInterface defined.
SBX-110490 | SBX-113016	2	PortFix SBX-110490: The IMS preconditions are failing due to UPDATE message race condition. **Impact:** An UPDATE from the calling party is queued by the SBC because the SBC is waiting for 200 OK for the previous update sent to called party, and when the 200 OK is received, the SBC did not forward the queued Update. **Root Cause:** Precondition parameters received as part of UPDATE from ingress endpoint is not updated in the egress CCB. **Steps to Replicate:** 1. Configure preconditions to transparent on both legs. 2. Configure transmitpreconditions to supported on both legs. 3. Run the script so that there is difference in precondition parameters in an INVITE and UPDATE messages from ingress. invite: a=des:qos mandatory local sendrecv a=curr:qos local none a=des:qos optional remote sendrecv a=curr:qos remote none (AS script)183 in Progress: a=curr:qos local sendrecv a=curr:qos remote none a=des:qos optional local sendrecv a=des:qos mandatory remote sendrecv a=conf:qos local sendrecv (IAD script)update : a=curr:qos local sendrecv a=curr:qos remote sendrecv a=des:qos mandatory local sendrecv a=des:qos optional remote sendrecv 4. Send the update from the Ingress when the SBC is waiting for 200 of the previous update it sent to egress. Verify that the SBC sends the queued update, once it receives the 200 ok for the 1st update.	The code is modified so the precondition level of support was set to transparent on both legs in configuration. When the SBC receives precondition parameters as part of an UPDATE and preconditions are transparent, then the SBC saves the precondition parameters into the egress CCB. When the queued update message is being processed there is check for preconditions flag and comparison of precondition variables is done to send the update to called party. **Workaround:** Enable the "Disable media lockdown" flag in IPSP for egress leg so that the SBC does not send the first update.

SBX-109364 | SBX-111831	2	PortFix SBX-109364: The SBC ERE was unable to handle "sonusdomain.IP" as a keepalive response from DNS. **Impact:** The SBC ERE was unable to handle "sonusdomain.IP" as a keepalive response from DNS. **Root Cause:** A format Error (dns_rcode_formerr) return code of a DNS server was unable to whitelist a server that was block listed. The DNS server is not getting whitelisted from a block list since the Format Error (dns_rcode_formerr) return code is not handled in the code. **Steps to Replicate:** 1. Configure the ARS profile. 2. Make a DNS server query with invalid format. 3. Verify the alarm to check that the server is on a block list. 4. Check after sending an ICMP message,the server is on a permit list.	The code is modified to fix the issue. **Workaround:** None.
SBX-112429 | SBX-112818	2	Portfix SBX-112429: The NrmGetCallCount was returning max global callcount, instead of the current stable calls. **Impact:** The I-SBC sends the total (cumulative) number of stable calls instead of current stable calls to the SLB in its utilization message. This could result in the SLB dropping messages if it thinks the I-SBC has reached 100% utilization. **Root Cause:** The I-SBC was providing the wrong number of stable calls to the SLB. **Steps to Replicate:** 1. Bring up the SLB-ISBC setup. 2. Run a call load. 3. Check in the SLB about current utilization of the I-SBC.	The code is modified to provide the current number of stable calls in the utilization message to the SLB. **Workaround:** None.
SBX-111740 | SBX-112570	2	Portfix SBX-11174: The SBC takes 72 seconds to send BYE to transferor after call termination. **Impact:** The SBC is taking 72 seconds to send BYE to the transferor when the transferee disconnects before a transfer target accepts the call. **Root Cause:** One of the disconnect events towards transfer target is getting ignored in the call control state machine. As a result, a release timer of 70 seconds is getting triggered later and the SBC is sending BYE towards transferor. **Steps to Replicate:** 1. A and B call is connected. 2. B sends a REFER to the SBC. 3. The SBC sends a new INV to transfer target C. 4. C sends 180 Ringing to the SBC. 5. A sends BYE to the SBC before C answers the call.	The code is modified so that the SBC sends a disconnect immediately towards the transferor. **Workaround:** None.
SBX-98627 | SBX-113514	2	PortFix SBX-98627: The Min-SE header is getting added to the ingress metaDataProfile even though it is not in the initial INVITE. **Impact:** For the SIPREC, the Min-SE and Session-Expires headers are added to the metaDataProfile even though it is not received in the initial INVITE. **Root Cause:** When receiving an INVITE, the SBC was incorrectly inserted Min-SE and Session-Expires headers as part of an incoming INVITE. **Steps to Replicate:** 1. Configure the SIPREC set up and Min-SE and Session-Expires in sipRecMetadataProfile. 2. Receive an incoming INVITE without the support timer and no Min-SE, no Session-Expires.	The code is modified so if an incoming INVITE is missing support for a Timer, the SBC resets the value of the Min-SE and Session-Expires only if it is received. **Workaround:** Use the SMM to delete the Metadata in the SIPREC INVITE.

SBX-105688 | SBX-110152	2	Portfix SBX-105688: The TAP ID of an ingress target was not getting embedded in the CCID for IMSLI (both leg interception). **Impact:** When a call has matched the ingress and egress LI criteria/target for a SIP Out of Dialog message and if each of the criteria was configure with different TAP IDs over the X1 interface, only one of the TAP IDs was processed by the SBC. This resulted in an incorrect TAP ID being sent out for one of the intercepted leg in the Correlation-ID (CCID) and in the TAP ID AVP field (202) of the X2 messages. **Root Cause:** The SBC always stored only one TAP ID, the TAP ID present in the 0th index of the LI criteria table that is returned by the PSX and it did not store the TAP IDs corresponding to ingress and egress criteria separately. As a result, whenever both legs are intercepted for OOD messages, one of leg would have the incorrect TAP ID in the CCID for X2 messages. **Steps to Replicate:** 1. Configure the SBC with the PSX and EMS for IMSLI Lawful interception. 2. Configure the IMSLI for both Leg and set targets using EMS with different TAP ID. 3. Make a subscribe request with the same targets configured. 4. Verify that TAP ID received for both legs are correct.	The code is modified to store and process the TAP ID for both the ingress and egress target criteria. **Workaround:** None.
SBX-109103 | SBX-111454	2	PortFix SBX-109103: There was an incorrect UDP port used in the Record-Route and Contact on the core side. **Impact:** The SBC populates an invalid port in the Contact/Record-Route header towards the IMS Core side in call progress (180/200) responses. **Root Cause:** The signaling engine in the SBC, during a call, progress command modifies the ports without validating the direction of message flow and causes the SBC to populate an invalid port in the SIP responses. **Steps to Replicate:** 1. Send an IMS-AKA registration request from a UE device. 2. Ensure the IMS-AKA registration is successful. 3. Let the registered user receive call from IMS network. 4. When UE accepts the call, we can observe in the call progress response sent from the SBC towards the IMS Core will have the invalid port in contact /Record-Route headers. Flow: IMS Core --(SIP UDP)-> SBC ---(SIP IPSec TCP)--> Peer (UE)	The code is modified to identify the direction before changing ports, change only when the flow is towards the UE. **Workaround:** Use the SMM to change the ports in Contact and Record-Route headers.
SBX-101255 | SBX-112998	2	PortFix SBX-101255: The OAM should not configure the same IP for two different pkt interfaces. **Impact:** The OAM is allowing the same IP and alternate IP to be configured under the same address context. **Root Cause:** During an address context, the interface creation OAM was allowing the configure of the same IP address (IpV4/IpV6) and alternate IP address for different interfaces. **Steps to Replicate:** The meta table is added for ipVarV4/ipVarV6/altIpVars value. When creating the ipInterface table, we should also observe ipInterfaceIpVarVMeta(hidden) The meta table is created for ipVarV4/ipVarV6/altIpVars. For all test cases, the following table can be observed: Case 1: Create ipInterfaceGroup,ipInterface and assign ipVarV4 Create 2nd ipInterfaceGroup,ipInterface and assign same ipVarV4 value, confd should throw an error for unique value in a address context. Case 2: Create ipInterfaceGroup,ipInterface assign ipVarV4 and altIpVars same as the one in ipVarV4 should throw an error for unique value. Case 3: Create ipInterfaceGroup,ipInterface assign ipVarV4 and altIpVars Create 2nd ipInterfaceGroup,ipInterface assign ipVarV4 and same altIpVars value as previous confd should throw error for unique value. Case 4: Create ipInterfaceGroup,ipInterface assign ipVarV4 and altIpVars Delete ipInterfaceGroup,ipInterface ipVarV4 Delete ipInterfaceGroup,ipInterface altIpVars Delete ipInterfaceGroup,ipInterface All combination of delete should work Case 5: The same test to be done for ipVarV6. Any other tests are related to ipVarV4/ipVarV6/altIpVars creation/deletion	The code is modified to have a unique IP address (IpV4/IpV6) and alternate IP address for an address context. New meta data is created for validating uniqueness efficiently. **Workaround:** Do not configure the ipVarV4/ipVarV6/altIpVars

SBX-111019 | SBX-113030	2	PortFix SBX-111019: The SBC should not allow to configure the same IP for two different pkt interfaces. **Impact:** The SBC should not allow to configure same IP for two different pkt interfaces. **Root Cause:** After a playback file pushed to the SC nodes, the dummy validate is invoked before creation of the addresscontext table, ipInterfaceIpMetaVar table to be moved out of addresscontext yang. **Steps to Replicate:** The meta table is added for ipVarV4/ipVarV6/altIpVars value. When creating the ipInterface table, we should also observe ipInterfaceIpVarVMeta(hidden) The meta table is created for ipVarV4/ipVarV6/altIpVars. For all test cases, the following table can be observed: Case 1: Create ipInterfaceGroup,ipInterface and assign ipVarV4 Create 2nd ipInterfaceGroup,ipInterface and assign same ipVarV4 value, confd should throw an error for unique value in a address context. Case 2: Create ipInterfaceGroup,ipInterface assign ipVarV4 and altIpVars same as the one in ipVarV4 should throw an error for unique value. Case 3: Create ipInterfaceGroup,ipInterface assign ipVarV4 and altIpVars Create 2nd ipInterfaceGroup,ipInterface assign ipVarV4 and same altIpVars value as previous confd should through error for unique value. Case 4: Create ipInterfaceGroup,ipInterface assign ipVarV4 and altIpVars Delete ipInterfaceGroup,ipInterface ipVarV4 Delete ipInterfaceGroup,ipInterface altIpVars Delete ipInterfaceGroup,ipInterface All combination of delete should work Case 5: The same test to be done for ipVarV6. Once saveAndActivate is called data should reflect in SBC as well. Case 6: Upgrade testing to be performed like from 9.x to 10.x. case 7: error case for upgrade testing, configure ipVarV4/ipVarV6/altIpVars and use same values for different ipInterface within an address context and post upgrade should get an error log for contacting sonus customer service to make the values unique. Run any tests related to ipVarV4/ipVarV6/altIpVars creation/deletion	The code is modified to move ipInterfaceIpMetaVar out of addresscontext yang. **Workaround:** None.
SBX-111956 | SBX-113152	2	PortFix SBX-111956: An early media case in SIPREC re-INVITE is not triggered with latest values for metaDataSource=fromLatest. **Impact:** Call modification events like codec change/hold/un-hold on the CS that occur before the RS Session is established is not propagated to the RS Call (SIPREC Session). **Root Cause:** The SBC does not attempts to trigger SIPREC re-INVITE with updated session characteristics when initial SIPREC INVITE transaction itself is pending with SRS and Main Call received a re-INVITE. **Steps to Replicate:** Run the following procedure to recreate the scenario: • Main Call (CS) session established. • SIPREC INVITE (RS) is sent towards SRS. • SRS does not respond for SIPREC INVITE. (SBC - SRS INVITE transaction is pending). • CS call goes for modification with RE-INVITE. (Hold/Codec change). • SRS answers the initial SIPREC INVITE after Main CS Call RE-INVITE.	The code is modified to queue the SIPREC RE-INVITE event when an initial SIRPEC INVITE transaction is pending. When the initial SIPREC INVITE transaction is completed, the queued SIPREC RE-INVITE is sent towards the SRS (This contains the latest session characteristics). **Workaround:** None.
SBX-110985 | SBX-111275	2	PortFix SBX-110985: If the VM name in the upper right corner of the "Configuration Manager" EMA/EMS SBC Manager is clicked, the browser freezes. **Impact:** If the VM name in the upper right corner of the "Configuration Manager" EMA/EMS SBC Manager is clicked, the browser freezes. **Root Cause:** The issue occurred because the peer setup was unreachable and to get the peer system info, the curl command that is executed was taking default timeout to get a connection timeout. **Steps to Replicate:** 1. Log into EMS. 2. Launch the SBC Node. 3. Click on **Monitoring** -> **System and Software info tab**.	The code is modified to address the issue. **Workaround:** Refresh the UI page.

SBX-112082 | SBX-112551	2	Portfix SBX-112082: There was an runtime error: member access within null pointer of type 'struct CC_SG_ALERTING_UIND_MSG_STR in CcSgAlertHndl. **Impact:** Run a basic G711U pass-thru call. After the call got completed, ASAN runtime error is observed in the system logs indicating that the code is taking the address of a field within a null pointer. This could potentially lead to coredumps if using the SIP recording capabilities other than SIPREC. **Root Cause:** When a call Progress/Alerting message is received from the network, the code was taking the address of a field within the pointer. **Steps to Replicate:** Run a basic call.	The code is modified to validate that the pointer is not null taking the address of a field within the pointer. **Workaround:** None.
SBX-113278 | SBX-113572	2	PortFix SBX-113278: Need a configurable item added to indicate a legacy meshed network on GW link to lower MAX_ICM value **Impact:** A call sent from an SBC running 9.0 or above to a older GSX may cause the GSX to core. **Root Cause:** In 9.0, the PDUs sent from the originating GW to the destination GW in a GW-GW call has increased in size. When the destination GW is an older GSX, the PDU may be larger than the buffer allocated on the GSX for receiving this PDU. In this case, the GSX does not expect a PDU this large and this will result in the GSX overwriting the allocated buffer causing memory corruption that eventually leads to a core. **Steps to Replicate:** Send an SBC-GW-GW-GSX call involving text (T140) streams. As a result, the GSX may crash. To test the fix: 1. Load the new code. 2. Enable oldGsxSupport "set global signaling oldGsxSupport" 3. Send an SBC-GW-GW-GSX call involving text (T140) streams (this is just 1 way to cause the large PDU to be sent). The GSX should not crash.	The code is modified so the new configuration parameter is enabled if there are any older GSXs in the network: set global signaling oldGsxSupport When this parameter is enabled, the SBC reduces the max size of the PDUs that can be sent over a GW-GW connection to older GSXs and older SBCs. **Workaround:** There is no workaround.
SBX-112708 | SBX-113492	3	PortFix SBX-112708: The NOTIFY XML body for 200 OK for INVITE does not contain new values that were updated between 180 and 200. **Impact:** The SBC was not sending latest received P-Asserted-Identity in the call NOTIFY XML body. **Root Cause:** The SBC was not considering the latest received P-Asserted-Identity and was always sending the first received message in call NOTIFY XML body. **Steps to Replicate:** Steps: 1. Enable the call Notification feature both legs. 2. Send different PAI headers in the 18x and 200 OK. Expected Result: The SBC sends ringing NOTIFY with the XML body contains PAI element that received in 18x and while sending a connected NOTIFY should consider PAI received in 200 OK.	The code is modified to consider the latest received P-Asserted-Identity identity for populating a call NOTIFY XML body. **Workaround:** None.
SBX-110997 | SBX-111367	2	PortFix SBX-110997: There are media problems due to same SSRC after hold /MOH/resume and a previous fix's flag was not helping. **Impact:** The SBC is not changing local SSRC during a HOLD/RESUME of a Transcoded call. **Root Cause:** During a HOLD/RESUME of a Transcoded call, the NP was not updated with the new SSRC generated by the SBC, and this resulting in the old SSRC being used in media packets. **Steps to Replicate:** 1. Run a basic Basic transcoded HOLD/RESUME SRTP call with the flag enabled. 2. Ensure that during a HOLD, only data-path-mode is changed to sendonly and recvonly respectively to trigger modify scenario and rest of the media attributes remains same. 3. Validate the media packets for change in the SSRC.	The code is modified to update NP with the latest SSRC generated during mid-call modification due to HOLD/RESUME of Transcoded calls. **Workaround:** If possible, switch to pass-through calls since this issue is specific to transcoded calls only.

SBX-113048 | SBX-113389	2	PortFix SBX-113048: Edited the External IP Interface group name disappearing in Visual First Call View as a diagramSetup. page **Impact:** Edited the External IP Interface group name disappearing in Visual First Call View as a diagramSetup page. **Root Cause:** The existing system did not handle save functionality when an external "IP Interface Group" was not empty. **Steps to Replicate:** 1. Login to EMA as an admin user. 2. Go to **Configuration**->**Configuration Wizards**->**Visual First Call Setup**. 3. Configure the fields in Carrier and save. 4. Make changes to IP Interface Group and Save. 5. Navigate to **All Admin** and then navigate back to **Configuration**->**Configuration Wizards**->**Visual First Call Setup** After navigating back to Visual First Call Setup, the changes were saved i.e. Carrier type and IP Interface Group should be visible.	The code is modified for the External "IP Interface Group" for both empty and non-empty cases. **Workaround:** None.
SBX-111721 | SBX-111722	2	PortFix SBX-111721: The EVS encoder picks up the initialCodecMode as the bitrate after switch to Compact Format. **Impact:** The EVS encoder picks up the initialCodecMode as the current bitrate if a change in packet format from Header Full to Compact is triggered. **Root Cause:** The root cause is the re-initialization of EVS encoder with bitrate as the initialCodecMode on change in packet format. **Steps to Replicate:** 1. Run a EVS<=>AMRWB call. br=5.9-24.4; bw=nb-wb 2. Stream a WB pcap with 13.2Kbps packets with CMR byte for 13.2 CA mode for the first 10s. After, the pcap has 24.4 Kbps packets without the CMR. Results: The mode of operation changes from 24.4Kbps to 13.2 Kbps with CA enabled on receiving the CMR. Once the Endpoint starts sending 24.4 Kbps packets without CMR, the SBC switches to Compact Mode while maintaining its bitrate as 13.2 Kbps with CA enabled. Prior to the fix, when switching to the Compact mode, the SBC would use 24.4 Kbps (initialCodecMode) as the bitrate.	The code is modified to the re-initialize the EVS encoder with bitrate as the localCodecMode rather than the initialCodecMode. **Workaround:** None.
SBX-111896 | SBX-112373	2	PortFix SBX-111896: Automatic daily updates in HFE script for Azure/GCE were causing the network to reset. **Impact:** Networking on the HFE can be reset by automatic updates. **Root Cause:** Ubuntu, by default, has an automatic package updater. Some package upgrades can cause the networking to be reset on the HFE node. **Steps to Replicate:** Check if the following timers are enabled: • sudo systemctl status apt-daily.timer • sudo systemctl status apt-daily-upgrade.timer	The code is modified to disable the timer that triggers the automatic updates. Package upgrades should only occur out of hours. **Workaround:** Run the following commands to disable the the updates: • sudo systemctl stop apt-daily.service • sudo systemctl stop apt-daily.timer • sudo systemctl stop apt-daily-upgrade.timer • sudo systemctl stop apt-daily-upgrade.service • sudo systemctl disable apt-daily.service • sudo systemctl disable apt-daily.timer • sudo systemctl disable apt-daily-upgrade.timer • sudo systemctl disable apt-daily-upgrade.service
SBX-110291 | SBX-112568	2	Portfix SBX-110291: AddressSanitizer: The ASAN detected a heap-buffer-overflow-SipSgIncomingCallNfy (unsigned int, sip_addr_str*, sip_msgbody_str*, sip_options_str*, unsigned int, unsigned int, bool) /sonus/p4/ws/jenkinsbuild /sbxAsan100/marlin/. **Impact:** The ASAN detected "AddressSanitizer: heap-buffer-overflow" while copying the contents of the SIP-I base version string internally. **Root Cause:** The SIP code was always copying a fixed amount of memory when reading the SIP-I base and version strings to internal memory. **Steps to Replicate:** Run a SIP-I call flow with INVITE and CANCEL messages.	The code is modified to copy exactly string length size of the SIP-I base and version content to avoid reading past the end of memory buffers as this can cause coredumps. **Workaround:** None

SBX-105367	2	During a sRTP and fax call, the sRTP context is removed for G711 fax pass-thru. **Impact:** The sRTP context is removed on the leg that has a G711 fax when there is a t38 to g711 fax call. **Root Cause:** The sRTP context is not updated for G711-fax. **Steps to Replicate:** 1. Run an A(SRTP)-B(RTP) CALL. 2. Run a leg A is G711 fax and B is T38. B sends a re-INVITE with t38 fax. 3. Check the re-INVITE that goes out with SRTP to endpoint A. 4. A party sends 200 ok with SRTP. 5. End the call.	The code is modified so the the SRTP context is updated only if the calleg has G711 fax. **Workaround:** None.
SBX-112905	2	The SBC was answering on-hold call with the sendrecv then re-inviting. **Impact:** On an incoming INVITE onhold, the SBC responds to the 18x offhold and later the re-INVITE onhold. **Root Cause:** There was a logical error that converts from an inactive to sendrecv when the first 18x is sent out. This issue was introduced a previous fix listed in the 9.2.1 release. **Steps to Replicate:** On the ingress, configure the Minimize flag, and uncheck relay data path mode. Incoming Invite onhold, egress response 18x. The SBC send 18x to ingress with sendrecv.	The code is modified to apply for subsequent 18x only. **Workaround:** Enable the relay data path mode.
SBX-110780	2	The SBC was sending Empty Packets when playing an Announcement. **Impact:** Announcement packets are empty for two stage calls if the NAPT enabled on the ingress. **Root Cause:** The ARM was not getting indication to start the announcement once NAPT learning was complete. **Steps to Replicate:** Set up a two stage call and enable the NAT on ingress.	The code is modified to send an indication to start the announcement once NAPT learning was complete **Workaround:** Disable the NAT.
SBX-111349	2	An SBC 7000 dual crash within 1 minute (old Active side - Fm, new Active - Scm). **Impact:** The application on both active and standby switched over and the application reset in a short order of each other. Core files are created on both sides of the HA pair. **Root Cause:** The issue occured during multiparty call processing where the SBC tries to determine a whether message was sent for the ingress or egress call segment. The code was accessing the pointer to the multi party call resource after it was freed up and set to NULL. **Steps to Replicate:** This issue is not reproducible. Potentially due to a race condition in the code.	The code is modified so the multi party call pointer is not NULL before reading from it to avoid the coredump. **Workaround:** There is no known workaround for this issue.
SBX-112953	2	The SRTP license counter did not incremented when the called side omits an SIP 18x response. **Impact:** The license count for the SRTP license was not updated on a call from SRTP to RTP, if no 18x response message is received. **Root Cause:** The SRTP license usage is not updated at the ingress when response to an INVITE is only 200 OK message. Therefore, if the egress is not using a SRTP, the call does not consume a license. **Steps to Replicate:** Make an SIP-SIP call where the ingress leg uses SRTP and egress leg uses RTP. The called side does not sent any 18x response.	The code is modified to correctly update the license count at ingress, even when no 18x is sent. **Workaround:** None.

SBX-110359	2	No INFO Logging Warning is provided when enabling the info debug/sys. **Impact:** The SBC CLI/EMA does not provide any warning when enabling INFO logging, indicating impact to system performance and call processing. **Root Cause:** There was no code to provide the warning to user. **Steps to Replicate:** Run the following script to reproduce the issue: admin@sbxsus12% set system admin sbxsus12 cliSetWarningOnEnablingInfoLevelLogging [disabled,enabled] (disabled): enabled [ok][2021-08-19 17:12:13] [edit] admin@sbxsus12% com Commit complete. admin@sbxsus12% set oam eventLog typeAdmin debug filterLevel info [ok][2021-08-19 17:14:51] [edit] admin@sbxsus12% com The following warnings were generated: 'oam eventLog typeAdmin': Enabling INFO level logging can be service impacting. Do you want to continue? Proceed? [yes,no] no Aborted: by user [ok][2021-08-19 17:15:41] [edit] admin@sbxsus12% com The following warnings were generated: 'oam eventLog typeAdmin': Enabling INFO level logging can be service impacting. Do you want to continue? Proceed? [yes,no] yes Commit complete. [ok][2021-08-19 17:15:46] admin@sbxsus12% set oam eventLog typeAdmin system filterLevel info [ok][2021-08-19 17:16:37] [edit] admin@sbxsus12% com The following warnings were generated: 'oam eventLog typeAdmin': Enabling INFO level logging can be service impacting. Do you want to continue? Proceed? [yes,no] yes Commit complete. [ok][2021-08-19 17:16:40]	The code is modified to provide a warning to the user when enabling INFO level logging for system or debug logs. To maintain backward compatibility and not break any customer scripts, a user needs to enable this extra prompt. **Workaround:** None.
SBX-112060	2	STIR/SHAKEN services were failing in the second dip in 2-stage call (SIP-SIP). **Impact:** The SBC was not sending STIR/SHAKEN parameters, such as identity headers, to the PSX in the trigger request portion of a two-stage call or processing the STIR/SHAKEN parameters in the response. **Root Cause:** The SBC was missing code to handle the interaction between two-stage calls and STIR/SHAKEN logic. **Steps to Replicate:** Make a two-stage call where the INVITE contains identity headers and check they are sent to the PSX in both the policy request and trigger request.	The code is modified to send STIR/SHAKEN parameters such as identity headers to the PSX in the trigger request portion of a two-stage call and process the STIR/SHAKEN parameters in the response. **Workaround:** None.
SBX-110746	2	The SIP ACK was missing in TRC, although the SBC sent one. **Impact:** The 200 OK for the INVITE received on the egress call leg contains a Record-Route header with an FQDN. The SBC resolves the Record-Route FQDN through the DNS and routes the ACK to the resolved target. The SIP ACK PDU that the SBC sent to the egress call leg is missing in the TRC log. **Root Cause:** The root cause is in SipsDnsLookupRspForTCB() when the DNS response comes back. SIP_CALL_STR *pstCall is set as NULL when SipsTXNDownstreamMsgToFsm is called. Due to the NULL check of pstCall in later functions, the SipSgTraceDumpSipPdu() is not called to log ACK PDU in TRC log. **Steps to Replicate:** 1. Set up: SIP-SBX-SIP. 2. Create a dnsgroup and configure the external DNS IP Address. Attach dnsgroup with egress zone. 3. Create a global calltrace filter with "level1" and key "calling". 4. Start the global calltrace and roll trace log event. 5. Run SIP-SIP call. 200 OK for the INVITE received on the egress call leg contains Record-Route with an FQDN. 6. Verify that egress ACK PDU is logged in TRC log.	The code is modified so in the function SipsDnsLookupRspForTCB, SIP_CALL_STR* pstCall is fetched and use in SipsTXNDownstreamMsgToFsm. **Workaround:** None.

SBX-109614	2	There were Error logs in DBG file after upgrade on 9.2.1 **Impact:** The SIPFE was reporting two kinds of major level error messages in the DBG logs: 1. port range id not found from SipFePortRangeCnxSendDataReq() e.g. SipFePortRangeCnxSendDataReq 366] PORT_RANGE: id not found 412765 2. port range id not found from SipFeRedundMirrorHashSync() e.g. SipFeRedundMirrorHashSync 1372] PORT_RANGE: failed to find Connection id in HAsh[4194719] **Root Cause:** Port Range Support was added in a previous feature that involves four subsystems, SIPSG, SIPFE, SIPCM and XRM, among 3 processes. There were several message exchanges between the four subsystems before a port range connection is fully established. Under certain circumstances, it is possible to hit some race conditions and find major DBG messages in DBG logs. **Steps to Replicate:** The steps cannot be replicated.	The code is modified to print extra call related data in the current major level debug messages to help triage more if the problem occurs in the future. When the issue occurs again, the call ID, signaling port Id, etc., is collected to help identify the call. The SipFeRedundMirrorHashSync() log is reduced from MAJOR level as well. **Workaround:** N/A
SBX-111541	3	Reloading previous configuration fails when the LDAP delayedSync is enabled. **Impact:** The delayed sync leaf used to accept only a future time if a configuration export and import is performed and if the system time is greater than the delayed sync time during import than import fails. **Root Cause:** The delayed sync leaf used to accept only a future time if a configuration export and import is performed and if the system time is greater than the delayed sync time during import then import fails. It fails due to the check on the delayed sync leaf value that should be greater than the current system time. **Steps to Replicate:** Use the following configuration: 1. Add a profile with a future time value on the delayed sync leaf. Export the configuration. 2. Clear the db. 3. Import the configuration when the system time is greater than the configured delayed sync time. 4. Import would fail without this fix.	Remove the restriction on the delayed sync leaf to be greater than the current system time to address the issue. **Workaround:** Modify the delayed sync time in the export CLI.
SBX-112267	2	Correct the 92x serialization code for a registration control block. **Impact:** When the registration control block is made redundant and the active /standby instances are running different software releases e.g. during upgrade, the redundancy logic might not work correctly if the registration control block contains a P-Charging-Vector (PCV) and/or P-Charging-Function-Addresses (PCFA) information. The redundancy logic will work correctly post upgrade when serialization of the redundancy data is not required. **Root Cause:** The parameter lengths of the PCV and PCFA redundant parameters was not calculated correctly. This can lead to the redundancy code being unable to process all the redundancy information correctly. **Steps to Replicate:** Run registration related tests with PCV and PCFA header parameters in an older release and then upgrade to 922R2 or later.	The code is modified to correctly set the length of these parameters to avoid problems with redundancy. **Workaround:** None.
SBX-112493	2	The SBC is not decrypting the IPsec packet when a large PDU was sent over IPv6 from Strongswan. **Impact:** The SBC is not decrypting the IPsec packet when a large PDU was sent from Strongswan IPSec endpoint. **Root Cause:** The SBC SWe NP has a issue in last fragment data length processing w.r.t. This StrongSwan fragmented first and encrypted the next combination IPSec packets handling, which caused an ESP trailer offset being incorrect and resulted in call failures. **Steps to Replicate:** Make large SIP PDU calls with the StrongSwan IPSec endpoint.	The code is modified to work for all combinations. **Workaround:** Racoon/Navtel/SBC IPsec endpoints can be used if possible as a workaround.
SBX-113546	2	Policy server transactions were failing while running a load (3xx redirection with light dip) with 75K Number Translation criteria. **Impact:** The postgres db is utilizing more CPU when a dmpm translation is executed at the service layer and as a result, impacting the performance. **Root Cause:** Using a dmpm rule, either the calling or the called number can be modified at the prerouter layer. The PES previously analyzed the called and calling number completely even though it was exclusive to the called number or the calling. During an analysis of the call, the PES used to perform direct DB fetch operations and this caused the postgres process to use more CPU. **Steps to Replicate:** Create a dmpm rule service to modify the calling number. And then perform performance testing. The postgres process will utilize more CPU.	The code is modified so that, the PES analyzes either only the called number or only the calling number based on the rule type. **Workaround:** none.

SBX-113610	2	A PES Process coredumps when deleting an adProfile entry. **Impact:** The PES Process dumps core when the AD profile is deleted. **Root Cause:** While synchronizing the data from remote domain controller, the PES fetches the AD profile once from the cache and uses the object for various decision making. So, if the AD profile is deleted, the object reference becomes NULL, and it dumps core. **Steps to Replicate:** To create an AD profile, create its dependent profiles. 1. Create An AD Attribute Profile. set profiles adAttributeMapProfile DEFAULT_AD_ATTRIBUTE_PROFILE adAttributeList adAttribute1 adAttributeName cn set profiles adAttributeMapProfile DEFAULT_AD_ATTRIBUTE_PROFILE adAttributeList adAttribute2 adAttributeName displayName commit 2. Create a domain controller profile set global servers domainController dc0 userName DcUsername password DcPassword primaryAddress DcIpAddress searchScope base=engineering, dc=some,dc=com ldapQueryCriteria cn=* commit 3. Create an AD profile: set profiles adProfile DEFAULT_AD_PROFILE delayedSync 2021-09-29T14:00:00 syncInterval 1440 sync enable adServerList 1 dcServer dc0 commit After 1-2 minutes of creating the AD profile, delete it.	The code is modified so the AD profile is not deleted. If, for some reason, the synchronization needs to be stopped, the sync opotion can be disabled on the AD profile. **Workaround:** If the AD profile is no more required, do not delete the AD Profile but disable the sync option on it. It will stop all the future auto sync operations.
SBX-112603	2	SBX-107111: Configured the DM/PM Rule not getting executed when the system is loaded with 75,000 number Translation criteria. **Impact:** When there are more than 3,000 number translation criteria (NTC) objects are created, the PES cache goes for rebuild of the entire cache. The cache rebuild was not caching the NTC objects correctly. **Root Cause:** During a rebuild of the NTC cache, a static variable was not reinitialized to zero. Since the static variable was not initialized to zero during a cache rebuild, it was using the last modified value, and this was causing the cache to not rebuild with the all the NTC objects. **Steps to Replicate:** Create more than 3,000 NTC objects and make a call to match the NTC key. It will fail to find a match in the cache.	The code is modified to initialize the static variable to zero, when a fresh cache rebuild is triggered. **Workaround:** None.
SBX-112670	2	The SBC is sending an unexpected INVITE towards the UAS. **Impact:** In an SBX-GW-GW-SBX call flow (as described in the test setup), the SBC was sending unexpected re-INVITE to the network. The re-INVITE was internally generated in order to handle the change in SDP parameters triggered by the SMM rules. **Root Cause:** This was a side effect of for a previous fix in the 9.2.1 release. **Steps to Replicate:** 1. Create a GW-GW set up. 2. From UAS send 183 with a=sendonly along with image and text lines with sendrecv. 3. SBC sends 183 with audio line as a=sendonly (That is removed by the SMM). 4. Send a 180 from the UAS that the SBC sends to UAC. 5. Send a 200 from UAS without the sdp. 6. The SBC sends a re-INVITE to ingress with audio m line sendonly along with image and text port as 0 (SMM changes the audio line to sendrecv). 7. The SBC gets 200 for re-INVITE from UAC with audio line sendrecv. After step 7, we should not see a re-INVITE towards the UAS.	The code is modified to take care of the case when holding a re-INVITE is actually received from a network or if it was locally generated. Only in a case where it was from network, we propagate the re-INVITE to the other end. **Workaround:** None.

SBX-113385	2	An unexpected 504 response was received, after a crankback to "500". **Impact:** When the SIP trunk group control UseNonDefaultCauseCodeForARSBlacklist is enabled and the outgoing message cannot be sent due to address unreachable status, the crankback to the next end point was not occurring. **Root Cause:** The code was incorrectly updated during 9.2.2 to try and map from SIP to CPC using internal 7xx status codes which are generated by the stack for events such as timeouts. This lead to the disconnect reason code being mapped to 0 that did not exist in the crankback profile instead of 168 which was expected. So the crankback did not occur and the call was released with 504. **Steps to Replicate:** 1. Run a test case with multiple trunk groups. 2. Send in a subscribe message that is routed through the SBC and respond back with 500. The message should be attempted to the next end point, but if that end point is blocklisted due to pathcheck configuration the message should be sent to the next again end point.	The code is modified to only consider the standard SIP status codes when trying to map from SIP to the CPC so that the correct disconnect reason code of 168 is used to trigger a crankback. **Workaround:** None.
SBX-113766	2	The SCM process crash was observed when trying to show the ARS blocklisted entries. **Impact:** When too many peers are in ARS blocklisted table(more than 90 entries) and the "show status addressContext default zone <ZONE_NAME> sipArsStatus" command was issued, the SCM process crashed. **Root Cause:** The code was incorrectly indexing to a negative location in an array that led to an invalid memory access and a coredump. **Steps to Replicate:** Block list multiple peers and then run the status command. This was only seen once in lab testing.	The code is modified to avoid accessing the negative array location to avoid the coredump. **Workaround**: None.
SBX-90989	2	EMA CDR Viewer: SIP Ladder diagram tool presenting incomplete packets The SBC CDR Viewer is enhanced to overcome SIP Ladder diagram size limitations to ensure large messages display. **Impact:** Incomplete packets display in the SIP Ladder diagram tool because the EMA did not know to append the next block to the previous PDU in the tool, and dropped the secondary packet block. **Root Cause**: Due to size limitations, large packets are getting split into two blocks, causing the second block to get prepended with information about the filter when it is written to the TRC log. **Steps to Replicate:** Use call trace filter to capture some large messages i.e. more than 2K in size and check that they are displayed correctly in the SIP ladder diagram.	The code is modified to ensure large messages display in the SIP Ladder diagram. **Workaround**: None.

Resolved Issues in 09.02.02R006 and 09.02.02R005 Releases

The following issue is resolved in these releases:

Table 15: Resolved Issues

Issue ID	Sev	Problem Description	Resolution

<table>
<tr>
<td>SBX-113278</td>
<td>2</td>
<td>The SBC is enhanced with a configurable parameter to indicate a legacy meshed network exists on the GW-GW links. This will ensure the MAX_ICM value used to pack a message to send to older GSXs is the same size.

Impact: A call sent from an SBC running software between 9.1.0 and 9.2.2R4 to any GSX (without the fix GSX-61814) may cause the GSX to core. The max buffer to send to the GSX was changed from 15K bytes to 10K bytes.

Root Cause: PDUs sent from the originating SBC to the destination GSX in a GW-GW network are bigger than the buffer on the remote GSX.

When the destination GW is a GSX, the PDU may be larger than the buffer allocated on the GSX. When the GSX encounters oversized PDUs, it overwrites the allocated buffer, causing memory corruption and ultimately a coredump may occur.

Steps to Replicate:

Send an SBC-GW-GW-GSX call involving text (T140) streams. The GSX may crash.

To test the fix:

1. Load the new code.
2. Enable the oldGsxSupport flag:
set global signaling oldGsxSupport enable
3. Send an SBC-GW-GW-GSX call involving text (T140) streams (this is just one way to send a large PDU).

The GSX should not crash.</td>
<td>The code is modified to add a new global signaling parameter that you must enable if there are any GSXs in the network without the fix for GSX-61814.

<code>set global signaling oldGsxSupport <disable | enable></code>

When this parameter is enabled, the SBC reduces the maximum size of the PDUs that can be sent over a GW-GW connection to GSXs to prevent sending a PDU larger than the buffer size allocated on the GSX, which can cause memory corruption. Once the GSX has fix for GSX-61814, it will send its maximum buffer size supported in the GW OPEN ACK (at which time you can disable this flag).

Any SBC running 9.1 or higher software supports this new AVP, and subsequently knows what to send to another SBC over the GW link. Calls will fail before getting cleared by the GSX with a 503, and will now fail on the ingress side with a 500 and advance to the next route.

<table><tr><th>New Flag</th><th>Description</th></tr><tr><td><code>oldGsxSupport</code></td><td>When the flag is enabled, the SBC reduces the maximum size of the PDUs sent over a GW-GW connection to a GSX to prevent the PDU sizes from becoming larger than the buffer size allocated on the GSX, which can cause memory corruption.

• <code>disabled</code> (default)
• <code>enabled</code></td></tr></table>
Workaround: There is no known workaround for this issue.</td>
</tr>
</table>

Resolved Issues in 09.02.02R004 Release

The following Severity 1 issue is resolved in this release:

Table 16: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-107747 | SBX-112648	1	PortFix SBX-107747: During Cyclic switchover tests, a PRS Process coredump was observed on the MSBC1. **Impact:** The application on both active and standby switched over and application reset in short order of each other. Core files were created on both sides of the HA pair. **Root Cause:** The issue occurs during multiparty call processing, when the SBC tries to determine whether a message was destined for an ingress or egress call segment. As a result of running multiparty call processing, the code was accessing the pointer to the multi party call resource after it was freed up and set to NULL. **Steps to Replicate:** This issue is not reproducible. Potentially due to a race condition in the code.	Check the multi party call pointer is not NULL before reading from it to avoid the coredump. **Workaround:** There is no known workaround for this issue.

SBX-112561 | SBX-112836	1	PortFix SBX-112561: The regexp string "\r\n" was not exported by “user-config-export”. **Impact:** The \r\n in regex is lost while exporting a configuration using the user-config-export CLI command. **Root Cause:** XML formatting trims empty node values. **Steps to Replicate:** 1. Create an SMM Profile using the following commands: set profiles signaling sipAdaptorProfile ESMM state disabled set profiles signaling sipAdaptorProfile ESMM advancedSMM disabled set profiles signaling sipAdaptorProfile ESMM profileType messageManipulation set profiles signaling sipAdaptorProfile ESMM rule 1 applyMatchHeader one set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 1 type message set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 1 message set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 1 message messageTypes requestAll set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 type header set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header name WWW-Authenticate set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header condition exist set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header numberOfInstances number 1 set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 2 header numberOfInstances qualifier equal set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 type parameter set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 parameter set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 parameter condition exist set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 parameter paramType generic set profiles signaling sipAdaptorProfile ESMM rule 1 criterion 3 parameter name realm set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 type header set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 operation regsub set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 headerInfo headerValue set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 from set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 from type value set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 from value 172.12.34.567 set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 to set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 to type header set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 to value WWW-Authenticate set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 regexp set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 regexp string "\r\n" set profiles signaling sipAdaptorProfile ESMM rule 1 action 1 regexp matchInstance all commit 2. Run the CLI command to the export configuration: user-config-export test.xml /profiles/signaling/sipAdaptorProfile 3. Delete the exported profile from CLI with the command: delete profiles signaling sipAdaptorProfile ESMM commit user-config-import test.xml 4. Run the following command: show configuration profiles signaling sipAdaptorProfile | display set | match string 5. Check if the regex string field, restores the original value.	Use the external XML tool called xmllint. **Workaround**: Manually edit the field in xml file after export.
SBX-112766	1	Details on "LAST RESTART REASON" under command "show table system serverStatus" are incorrect. **Impact:** The LAST RESTART REASON is not updated with a correct reason of last restart. **Root Cause:** Reading LAST TESTART REASON function is called twice and in second call, it is set to default. **Steps to Replicate:** Check the LAST RESTART REASON from CLI show table system serverStatus and call a different type of restart and verify LAST RESTART REASON set properly or not.	The code is modified to set the reading LAST TESTART REASON function to call only once. **Workaround**: None.

The following Severity 2-4 issues are resolved in this release:

Table 17: Severity 2-4 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-111349 | SBX-112883	2	PortFix SBX-111349: The SBC 7000 has a dual crash within 1 minute (old Active side - Fm, new Active - Scm). **Impact:** The application on both active and standby are switched over and application reset in short order of each other. Core files are created on both sides of the HA pair. **Root Cause:** Accessing a NULL pointer that leads to a coredump. **Steps to Replicate:** Test switchover scenarios to replicate the issue.	The code is modified to address the issue. The ccbPtr->ccMultiCallMsgStrPtr is checked for not being NULL. **Workaround:** None.

SBX-112857	3	The VNFM response is timing out due to the timeout value length. **Impact:** By default the VNFR logic had a 5-second timeout to get responses from VNFM for the REST requests that it sent, but it has been observed that in certain networks this timeout value is not enough. This lead to the VNFR timing out while the VNFM was still trying to send back a response and the VNFR never reported ready state in the VNFM. **Root Cause:** A 5-second delay was originally considered adequate, but after taking multiple networks into account, the delay proved to be insufficient. **Steps to Replicate:** Try a relocation operation with VNFM across multiple sites and ensure the VNFR status returns to ready.	The code is modified so the timeout is increased to 20 seconds. **Workaround**: None.
SBX-112493 | SBX-112785	2	PortFix SBX-112493: The SBC is not decrypting IPsec packet when large PDU sent over IPv6 from Strongswan. **Impact:** The SBC is not decrypting IPsec packet when large PDU sent from Strongswan IPsec endpoint. **Root Cause:** The SBC SWe NP has an issue in the last fragment data length processing. This StrongSwan was fragmented first and encrypted the next combination IPsec packets handling, which caused ESP trailer offset being wrong and call failures. **Steps to Replicate:** Make large SIP PDU calls with the StrongSwan IPSec endpoint.	The code is modified on the last segment length to work for all combinations. **Workaround**: The customer and the SBC IPsec endpoints can be used if possible.
SBX-112153 | SBX-112627	4	PortFix SBX-112153: An investigation found commits are not saved/activated on many SBCs. **Impact:** Warnings displayed about inactive configurations on the managed VM. **Root Cause:** The managed VM was checking the status on the OAM shared drive and reporting the inactive configuration warnings. **Steps to Replicate:** Test on OAM and manage the VM.	The code is modified to only display the warning on OAM nodes. **Workaround**: None.
SBX-112117	2	There is a Wall LRA ISBC switchover after the applying ACLs. **Impact:** Configuring certain combination of ACLs may exceed the hugepage requirement than available in the system. This will cause the ACL configuration to fail and SWe_NP to exit. **Root Cause:** The code did not account for available hugepages during an ACL configuration. **Steps to Replicate:** Bring up setup in ISBC profile. Apply the ACL configuration used by customer.	The code is modified to limit the hugepage memory use during an ACL build and ensure it is within the allocated limit. **Workaround**: Use more than 64G RAM.

Resolved Issues in 09.02.02R003 Release

The following issue is resolved in this release:

Table 18: Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-105370	1	The Active Register per TG shows more than the total stable registration. **Impact:** Under some condition(s), the ingress zone's activeRegs count can be incremented and not decremented when the registration terminates. The causes the ingress zone's activeRegs count to grow incorrectly, and never reach ZERO (even after all registrations are terminated). **Root Cause:** The SIPFE and SIPSG RCB allocation/deallocation become out of sync, indirectly causing the ingress zone's activeRegs count to increment and not decrement. **Steps to Replicate:** Perform REGISTER/401 - REGISTER/403 until the ingress zone activeRegs count issue is detected.	The code is modified to correctly handle the SIPFE's registration bind timer expiration. **Workaround:** None.

Resolved Issues in 09.02.02R002 Release

The following Severity 1 issues are resolved in this release:

Table 19: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution

SBX-111688 | SBX-112126	1	PortFix SBX-111688: The Request-URI and TO fields in a SIP INVITE are incorrect and overwritten. **Impact:** When the Diversion header presented in an Ingress INVITE and had no RN in Request-URI, the egress RURI would use the RN in username field, after a PSX LNP dip. **Root Cause:** The fix for a previous issue broke the previous RURI username setting. **Steps to Replicate:** 1. Set up the SBC with an external PSX to make LNP calls. 2. Pay attention to the disableRn flag in egress IPSP in PSX and flag UseGAPwhenRnisDisabled in the SBC's egress TG. Test different combination of < disableRn, UseGAPwhenRnisDisabled > 3. Ingress INVITE needs to contain Diversion header and no RN in the Request-URI. Sample message could be found in the reproduced DBG logs and finalFix DBG logs.	The code is modified to ensure the RURI always contains the correct username. **Note**: When the egress IPSP has "SIP TO Header Mapping" set to "Called Number", the TO header's username is the ingress TO URI. The number will not be globalized. If the customer would like it to be globalized, the globalization profile of the egress TG could be modified to globalize TO URI. Another way is using SMM to modify it. **Workaround:** Use the SMM and use the Warning-21-00029918
SBX-111223 | SBX-112194	1	Portfix SBX-111223: Memory leak since upgrading to 8.2.5 R0. **Impact:** High memory utilization. **Root Cause**: Two leaks of the same structure exist: 1. A memory leak is seen when a relayed SUSCRIBE message is cranked back and an Alternate Server cannot be found. 2. The code that handles relayed messages may cause a leak in certain error scenarios. Warning-21-00029922 pertains to this issue. **Steps to Replicate:** This is a memory leak that may be triggered if a relayed SUBSCRIBE is cranked back and then an alternate route is not found. 1. This memory leak that may get triggered if a relayed SUBSCRIBE is cranked back and then an Alternate Server is not found. 2. We were unable to reproduce this error scenario which causes a leak of the Relay Control Block.	1. The code is modified to take the correct path when an Alternate Server cannot be found while handling a relayed message that has been cranked back. 2. Code has been added to start a timer when we begin processing a relayed messsage. In error cases, the Relay Control Block will be free when the timer expires - preventing the structure from leaking. **Workaround:** None. Once the memory utilization reaches 91%, an automatic switchover occurs. To avoid an automatic switchover, Ribbon recommends performing a manual switchover during a low traffic period.
SBX-112309	1	An LSWU on SWe (VMware/KVM) through the Platform Manager fails with the additional reboot of the standby. **Impact:** An LSWU from 09.02.02R001 to any higher release 1:1 HA SWe (KVM/VMware) through the Platform manager fails because the standby instance undergoes an additional reboot during the upgrade procedure. **Root Cause:** The Index Marker file was missing on the standby instance prior to the LSWU procedure. The Index Marker file was missing on the standby instance due to when the application comes up with the standby role, the Index Marker is created only when there is a mismatch in the calculated and DB populated indices. **Steps to Replicate:** 1. Create 1:1 HA SWe on KVM/VMware. 2. After the HA application comes in sync, run clearDB on the standby. 3. Perform an LSWU on the 1:1 HA SWe.	The code is modified so the Index Marker file is created on the standby instance irrespective of processor index mismatch in the calculated and DB populated indices. **Workaround**: Before initiating the upgrade procedure (from PM or CLI), the user needs to run the following command as a root user from the linux shell of the active and standby instance. touch /opt/sonus/conf/swe/capacityEstimates/.indexMarker

SBX-112229	1	The term-ioi is not be set in the STOP record for a customer call flow. **Impact:** When running a JJ90.30 to JJ90.30 call flow, the term-ioi value from the PCV header is not being stored in the ingress protocol variant string when the transitPCV control in the JJ90.30 interworking profile is enabled. **Root Cause:** The original development work was only storing the term-ioi value in the egress protocol variant string. **Steps to Replicate:** Make JJ90.30 to JJ90.30 call. transitPcv is set to enabled in the customer's Interworking Profile. Call 1: INVITE --> (PCV with icid-value and orig-ioi) <--- 180 (PCV with icid-value, orig-ioi, term-ioi) <-- 200 OK (PCV with icid-value, orig-ioi, term-ioi) --> BYE Call 2: INVITE --> (PCV with icid-value and orig-ioi) <--- 180 (PCV with icid-value, orig-ioi, term-ioi) <-- 200 OK (PCV with icid-value, orig-ioi, term-ioi) <-- BYE After a call, verify the CDR records. In both START and STOP records, the term-ioi is filled in ingress PVSD.	The code is modified to ensure the term-ioi value is stored in the ingress protocol variant string. **Workaround**: None.
SBX-112381 | SBX-1124488	1	PortFix SBX-112381: The SBC had a Crash-Application in the rebooting loop. **Impact:** A PRS Process core is occurring when the code is processing an ICE STUN packet and there are more than 20 Teams clients ringing. This could potentially happen in a simultaneous call group pickup scenario. **Root Cause:** The root cause of the core is a bug in the code that handles the incoming STUN packet. This code is overwriting the end of array by writing too many entries into the array. This results in memory corruption and eventually a core. **Steps to Replicate:** Run a call group pickup scenario with more than 20 users all having their Teams clients ringing at the same time.	The code is modified to prevent it from writing too many entries into the array. **Workaround:** Disable media-bypass or reduce the number of users in the call group.

The following Severity 2-3 issues are resolved in this release:

Table 20: Severity 2-3 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-111751	2	The SCM Process is coredumping. **Impact:** The SBC is relaying multiple reason header instances in the amount of the quantity squared. **Root Cause:** Logical error when multiple instances of a reason header on the same line. The SBC is relaying in the amount of quantity squared. **Steps to Replicate:** 1. Configure the transparency Reason header. 2. Make a SIP-SIP call, Ingress sends BYE with multiples Reason header instances on the same line. The SBC sends instances in an amount of the quantity squared to the Reason header on Egress. **Note**: If the ingress sends a large number of instances on the same line. • For old (pre 8xx), the SBC may core. • For 8xx and above, the SBC may be unable to send BYE on Egress.	The code is modified to address the issue. **Workaround:** Disable the transparency of a reason header.

SBX-111932	2	A restore on revision 1 failed in the standby OAM node. **Impact:** A restore on revision 1 failed on the standby intermittently. **Root Cause:** When the restore revision is requested, both OAM nodes restart. In a corner case, there is possibility of both starting as active and later one of the nodes will go down and not come up as standby. **Steps to Replicate:** 1. Create a scenario with 1:1 OAM for the SSBC/MSBC/MRFP. 2. In automation, keep the cleanStart as 1 so that the automation will trigger restore revision 1. Both OAM should come up.	The code is modified to handle the corner case. **Workaround**: Manually reboot the standby.
SBX-112039	2	Uploaded onfig backup file is not available at gconfig. **Impact:** The uploaded config backup file is not available on the gconfig. **Root Cause:** The uploaded file was not moved in the config directory because the system name was not correct. **Steps to Replicate:** 1. Log in to the EMA. 2. Go to **Administration** -> **System Administration** -> **File Upload**. 3. Upload the file.	The code is modified to read the correct system name. **Workaround**: None.
SBX-112085	3	The SFTP transfer is not working to CDR server that only supports AES128_CTR. **Impact:** One customer has a CDR server that offers AES128_CTR for the server-to-client encryption. When the SBC offers AES256_CTR as the preferred option, the SBC encodes the packets with AES256_CTR, and receives the packets with AES128_CTR encryption. This scenario causes a decoding issue on the SBC that results in the termination of the connection. **Root Cause:** An invalid encrypted data length is received from the CDR server. **Steps to Replicate:** 1. Rollover the accounting file. 2. Verify that the CDR transfer is successful.	The code is modified to offer up the AES128_CTR as the preferred encryption option, so both sides are using AES128_CTR. **Workaround**: Disable the AES256 on the CDR server.
SBX-112267 | SBX-112332	2	PortFix SBX-112267: The correct 92x serialization results in test failures. **Impact:** When the registration control block is made redundant and the active/standby instances are running different software releases, the redundancy logic might not work correctly if the registration control block contains P-Charging-Vector (PCV) and/or P-Charging-Function-Addresses (PCFA) information. The redundancy logic will work correctly post upgrade when the serialization of the redundancy data is not required. **Root Cause:** The parameter lengths of the PCV and PCFA redundant parameters was not calculated correctly. This can lead to the redundancy code being unable to process all the redundancy information correctly. **Steps to Replicate:** Run registration related tests with PCV and PCFA header parameters in an older release and then upgrade to 922R2 or later.	The code is modified to correctly set the length of these parameters to avoid problems with redundancy. **Workaround**: None.
SBX-111659 | SBX-112378	2	PortFix SBX-111659: The intercept is not working when P-Com.Session-Info is received in INVITE and tones are enabled. **Impact:** When the lawful intercept target is specified in the P-com-session-info header of the INVITE message, the intercept does not occur if an announcement resource is applied to the call and then freed up. There is no issue if the P-com-session-info header is received in the backward direction. **Root Cause:** This occurs when using P-early-media with tone profile and media monitoring profile applied to the call flow and the B-party sends P-early-media with a=inactive to start the media monitoring and does not provide RTP or does not send 200 OK prior to the monitoring timer expiring which results in the SBC playing RBT via an announcement resource. When the media path is later cut through and the announcement resource is released the intercept information was mistakenly freed up and the intercept did not occur. **Steps to Replicate:** 1. Run a lawful intercept call flow using P-com-session-info header in the INVITE to indicate the target intercept point. The call should be configured with P-Early-Media, tone profile and monitoring profile to check for RTP packets received. 2. In response to the egress INVITE, send back an P-early-media header with a=inactive and no RTP packets prior to the monitoring timer expiring so the SBC plays RBT. 3. Answer the call and check that media is being sent to the intercept server.	The code is modified to ensure the intercept information is not freed up when freeing the announcement resource. **Workaround**: None.

SBX-112487	2	The LI connection to media server was not connected on a switchover. **Impact:** When using the PCSILI (P-com-session-info flavour of LI) in an N:1 M-SBC setup and running the SBC release 8.2 or later if there is a switchover, the connection to the LI server might not be re-established. **Root Cause:** The standby instance was trying to maintain information about the operational status of the interface used for LI processing. But this was only happening correctly for the first instance. The status of the other instances was being misinterpreted and lost. So during the transition to active, the LI code thought the interface was not available and did not try to establish the connection to the LI server. **Steps to Replicate:** In an N:1 setup perform switchovers from each active instance to the standby and check that the connection to the LI server is restored.	The code is modified to collect the status of the interface after the instance transitions from standby to active so that the accurate interface information is available for LI processing. **Workaround**: Bounce the interface e.g. ifup/ifdown that is used for LI connection would help to recover the connection.

Resolved Issues in 09.02.02R001 Release

The following Severity 1 issues are resolved in this release:

Table 21: Severity 1 Resolved Issues

	Issue ID	Sev	Problem Description	Resolution
1	SBX-108317 | SBX-111780	1	PortFix SBX-108317: The SBC switchover and isolation of node/SVWSBCD. **Impact:** The PRS core was truncated because a second ABRT was sent to the process. **Root Cause:** The PRS core was truncated because a second ABRT was sent to the process while it was in the process of writing the core. **Steps to Replicate:** This issue is not reproducible.	The code is modified to prevent two ABRT signals from being sent to the same process. **Workaround:** There is no workaround.
2	SBX-111050 | SBX-111595	1	PortFix SBX-111050: There was a coredump during a reboot on a customer SBC. **Impact:** A misconfiguration of GW Signaling Ports, in which there is a Secondary GW Signaling Port configured but no Primary GW Sig Port configured, and can lead to a core and switchover. **Root Cause:** When there is no Primary GW Signaling Port configured but there is a Secondary Signaling Port configured, we enter a code path that attempts to dereference a NULL pointer (pointer to Primary Sig Port) when it is attempting to get the dscp value to use for the socket. **Steps to Replicate:** An SVT engineer should: 1. Configure an SBC with a Secondary GW Signaling Port without configuring a Primary GW Signaling Port. i.e. gwSigPort of SBC1 should be in primary mode and SBC2 should be in secondary mode 2. Send a GW-GW call from a remote GW through this SBC using the address of the Secondary GW Signaling Port on an SBC. Without the fix, this should cause a core. With the fix, there should be no issue.	The code is modified to prevent it from attempting to dereference a NULL pointer (pointer to Primary Sig Port) when it is looking up the dscp value to use for the socket. **Workaround:** The workaround is to avoid configuring a Secondary GW Signaling Port without configuring a Primary GW Signaling Port.
3	SBX-110199 | SBX-111474	1	PortFix SBX-110199: There was dbg log flooding with MAJOR .VNFR: * (VAgent) message **Impact:** Event Logs are flooded with error message, when one of the OAM node or Managed VM goes down. Log Message:.MAJOR .VNFR: *(VAgent): send error. rc=-1, error=Resource temporarily unavailable **Root Cause:** The health check message send fails, when an instance is down. **Steps to Replicate:** Run an LSWU from VNFM on an ISBC SWE instance in 1 to 1 HA mode.	The code is modified so the messages are only logged on the first error in health check. It is reset, when a message send succeeds. **Workaround:** The error message stops automatically once the node is recovered and starts to respond to the health check messages.
4	SBX-110884 | SBX-111318	1	PortFix SBX-110884: The logs are getting printed in openclovis. **Impact:** If condition present, SCM is filling openclovis logs with this error message: nprintf buffer too small. Need 306 Have 300 File: /sonus/p4/ws/release /sbx5000_V08.02.02R001/marlin/SIPSG/sipsgRegAgent.c Line: 2527 **Root Cause:** The error message is being logged because the code is attempting to write a debug log into a local buffer that is not big enough. **Steps to Replicate:** No testing is required. This is no risk with/without fix.	The code is modified to increase the size of the local buffer. **Workaround:** There is no workaround.

5	SBX-109243 | SBX-111274	1	PortFix SBX-109243: The SBC sending 481 for CANCEL in dialog transparency. **Impact:** When the dialog transparency is enabled and call loops back to the SBC, the SBC does not handle a CANCEL sent from ingress endpoint. **Root Cause:** The SBC expects a CANCEL to have callinfo header. **Steps to Replicate:** 1. Reproduce the issue. Dialog Transparency is enabled and the Call Loops back In. After adding PRACK, Ingress sends CANCEL without callinfo header. The SBC sends a 481. 2. With a fix, the SBC sends 200OK for CANCEL and relays to egress leg.	The code is modified to ensure the SBC finds the correct SG to handle the CANCEL even when the CANCEL does not have callinfo **Workaround:** None.
6	SBX-111100	1	Host check validation failing - Required GB RAM 6 but found 0.03125. **Impact:** The few host machines in the AWS data center use different units for RAM, HostCheck script assumes that available memory is given in MB. The HostCheck script is fixed to calculate available memory based on unit of memory. **Root Cause:** The HostCheck script does not have code to consider memory unit. **Steps to Replicate:** Create VM with >=32 GB RAM, application should come up without complaining about memory in VM.	The code is modified to calculate available resources based on units. **Workaround:** Create instance/VM that has < 32 GB RAM.
7	SBX-107133 | SBX-111046	1	Portfix SBX-107133: Max FD limit is reached in SLB beyond 7,04,000 TLS co nnections (Access Registrations) tried. **Impact:** Max FD limit is reached in the SLB beyond 7,04,000 TLS connections (Access Registrations) tried. **Root Cause:** Observing the FD congestion at high load due to FD limits reached. **Steps to Replicate:** Check the updated FD limits in /etc/security/limits.conf.	The code is modified for the max FD for the KVM and SLB. **Workaround:** None.
8	SBX-110350	1	The SBC is forming invalid packet where it is adding 00 in around all headers and parameters. **Impact:** The SBC puts a NULL termination in every parameter and header of the message. In this case, there was a parser error on a parameter when the DNS translation was required. **Root Cause:** During the parsing of the message after a DNS query, if a parser error occurs, then incorrect termination is put/left in the message when sent on the wire. **Steps to Replicate:** 1. An incoming INVITE had a known syntax error related to alert_info, configuration was to parse through the filterProfile and not transparently forward alert_info. This resulted in parse error and bad formatting when DNS was executed. 2. Configure the alertInfo to transparently pass on egress, and DNS function doing fqd/IP swap executes correctly and egress message is sent with good formatting.	The code is modified to: 1. Log parse an error line number and pdu message. 2. Apply the filterProfile when parsing the message. The customer needed to add filterProfile to transparently forward the parameter failing parsing on egress to avoid parse error and avoid incorrect parameter termination. **Workaround:** On the Ingress, apply an SMM to rename alert_info to an unknown (x-alert_info), and rename back on the egress.

The following Severity 2-3 issues are resolved in this release:

Table 22: Severity 2-3 Resolved Issues

	Issue ID	Sev	Problem Description	Resolution
1	SBX-111394	2	The file upload is not working in the Platform Manager. **Impact:** The file upload is not working in the PM. **Root Cause:** The request URL length was too high as per-server configuration because that requested call was failed. **Steps to Replicate:** 1. Log in to the Platform Manager. 2. Go to **Administration** -> **System Administration** -> **File Upload**. 3. Upload a file and save it.	The code is modified to make a request call successful. **Workaround:** We can apply the same changes in a customer setup also and restart the apache server.

2	SBX-111700	2	Getting badRidCb errors during LSWU from 7.2.4R0 to 9.2.2A003 **Impact:** An upgrade from an older version to 9.2.0R0 and newer, the NP reported badRidCb error continuously: MAJOR .IPM: *NP 0 error counter badRidCb incremented: cnt 2310 last error 0x10002. **Root Cause:** In version 9.2.0R0, Ribbon Protect streaming support was added. During an LSWU, new fields related to Ribbon Protect streaming were all initialized to zero in internal data structures, including the rbbnType. But in NP, rbbnType = 0 triggered NP to send RTCP_APP related statistics to Protect server, which caused the errors. **Steps to Replicate:** Run an LSWU from any older version to 9.2.2 with call loads.	The code is modified to initialize the rbbnType to 'BRM_RBBN_PROTECT_STREAM_DISABLE' so that NP does not generate RTCP_APP to Protect server. **Workaround:** No workaround.
3	SBX-111211 | SBX-111652	2	PortFix SBX-111211 to 9.2.x - Get "violates foreign key constraint" error when assigning timeRangeProfile to a Route in EMA **Impact:** Route creation fails when the name of time range profile contains numerals. **Root Cause:** During the route creation, validation of time range profile was failing as it was containing numerals. **Steps to Replicate:** 1. Create a time range profile with a name containing number ex test_1 2. Create a route with test_1 as time range profile. 3. Route creation should be successful.	The code is modified to consider numerals as valid a character. **Workaround:** Create a Route from the CLI.
4	SBX-108616 | SBX-111571	2	PortFix SBX-108616: Fora Late Media Call, the SBC is not sending a second UPDATE towards ingress when the DLRBT is enabled. **Impact:** In a late media convert call scenario, when the DLRBT is enabled, the SBC is not sending UPDATE towards the ingress with the list of codecs received from UAS. **Root Cause:** The minimizing of media changes from other call leg functionality is suppressing the triggering of the UPDATE towards UAC. **Steps to Replicate:** 1. The UAC sends INV without SDP to the SBC. 2. The SBC sends INV with PCMA PCMU G729 101. 3. The UAS sends 180 with PCMA G729. 4. The SBC sends 180 with PCMA G729. 5. The UAC sends PRACK with G729. 6. The SBC starts playing tone with G729 towards ingress EP. 7. The UAS sends 200 OK (for INV) without SDP.	The code is modified to identify this particular call scenario, such that, the SBC sends an UPDATE towards the UAC if the tone codec is different from the end to end negotiated codec. **Workaround:** None.
5	SBX-111502 | SBX-111566	2	Portfix SBX-111502: Metavar exchange continues even after the allocation is failed in the SBC. **Impact:** The CHM processes the metavar request/response messages even when the application is going down, which results in failure messages. **Root Cause:** The CHM does not check if the application is going down while processing the messages from the other nodes. **Steps to Replicate:** Bring up the SBC in N:1 mode and then shutdown the application on one of the nodes while another node is starting the metavar exchange in CHM activation.	The code is modified to ensure that application is not going down before processing the metavar messages from other nodes. **Workaround:** None.
6	SBX-111469 | SBX-111565	2	Portfix SBX-111469: There are some problem causing MRFPs cannot recover from a restart **Impact:** The standby SBC gets the already allocated metavars of an active node while coming up in an 'active' role. **Root Cause:** The standby SBC is not checking for the condition to see if its the only node running in the redundancy group before allocating the last exchanged metavars of active node. **Steps to Replicate:** Bring up the N:1, trigger a switchover so that assigned standby becomes active and while assigned active node is coming up in 'standby' role. Restart assigned standby and ensure the proper metavars are allocated to assigned standby node while its coming up in 'active' role.	The code is modified to check for the already allocated metavars before allocating the metavars to self node while coming up in the 'active' role. **Workaround:** Restart assigned standby node if already allocated metavars are allotted to this node.
7	SBX-111310 | SBX-111562	2	Portfix SBX-111310: Standby OAM is rebooting after orchestration. **Impact:** The Standby OAM is restarting after a launch. **Root Cause:** The Standby OAM is sending the serf event for 'startingStandby' with an older timestamp (which is fetched even before standby OAM is ready to come up) that results in discarding of the serf event by the active OAM node as its prior to member-join event for standby OAM node. **Steps to Replicate:** Bring up both the active and standby OAM at the same time and then while standby OAM is coming up, disconnect and connect the HA port on active OAM to trigger member-failed and member-join events.	While sending the 'startingStandby' serf event, get the current timestamp so that its not discarded by the active OAM node. **Workaround:** Restart the standby OAM application so that the startingStandby event is generated again with a current timestamp.

8	SBX-109811 | SBX-111520	2	PortFix SBX-109811: The SBC uses port number RTP+1 for RTCP instead of the learned RTCP port number if the RTCP NAT learning completes before RTP NAT learning. **Impact:** The SBC sends the RTCP packets to a destination port number RTP+1 for the RTCP instead of the learned RTCP port number if the RTCP NAT learning completes before RTP NAT learning. **Root Cause:** The SBC overwrites the learned RTCP port number with the RTP+1 port number if the RTCP is learned before RTP. **Steps to Replicate:** Send RTCP packets first then RTP packets to the SBC. After call is connected, verify the RTCP port number, if RTCP is learned before RTP.	The code is modified to use correct RTCP learned port when RTCP learning occurs before RTP, instead of comparing the RTP and RTCP addresses from callLeg structure. **Workaround:** No workaround.
9	SBX-89177 | SBX-111468	2	PortFix SBX-89177: A call is torn down upon a Hold (OA expiry). **Impact:** A call flow involving an early media, tone and late Crankback results in a call tear down by the SBC while processing the HOLD INVITE. **Root Cause:** While processing a 200 OK for INVITE, one of the call processing module ends up setting wrong App-Context-Id as active. Later, while processing a HOLD INVITE, this causes a failure since this module is not working on the latest App-Context-Id. **Steps to Replicate:** Call Scenario: 1. Party A calls Party B through the SBC. 2. Party B sends 183 with SDP resulting in media cut-through at the SBC. 3. Later B sends 480. 4. The SBC is configured for the Crankback and as a result sends INVITE to Party C. 5. Party C sends 183 with SDP. 6. Party C sends 180 without SDP resulting in tone. 7. Party C sends 2xx with SDP for INVITE. 8. Party C sends HOLD INVITE. Expected behavior: The SBC successfully process the HOLD INVITE. Actual Behavior (without a fix): The SBC tears down the call while processing HOLD INVITE.	The code is modified to have the correct app Context Id as active while processing 200 OK for INVITE. **Workaround:** Disable the Tones at the SBC.
10	SBX-110948 | SBX-111397	2	PortFix SBX-110948: Load configuration overwrites the local processor index values. **Impact:** When we perform a load config operation on a 1:1 HA pair (SWe/Cloud), it ends up overwriting the local processor index estimates with the ones that are present in the config dump. This leads to two issues: 1. An incorrect index estimates being populated in the DB. 2. There are discrepancy in estimations between active and standby instances. **Root Cause:** The load config operation results in overriding the local processor index estimates with the ones that are present in the config dump. This results in standby consuming incorrect indices present in the DB thereby causing the discrepancy in estimates of the active and standby instances. The DB should always reflect the estimated processor indices calculated by the active instance in 1:1 HA pair. **Steps to Replicate:** On 1:1 HA SWe/Cloud instances, perform the following steps: 1. Run the following command as root user on the active and standby instances. The following command should give same output on the active and standby instances. cat /opt/sonus/conf/swe/capacityEstimates/.index.txt 2. Perform the load config operation. 3. Run the following command as root user on the active and standby instances. The following command will give different output on the active and standby instances. cat /opt/sonus/conf/swe/capacityEstimates/.index.txt With the fix, this issue will not be observed.	The code is modified to ensure that the DB reflects the estimated processor indices calculated by the active instance in 1:1 HA pair. If the processor indices values stored in the DB does not match with the indices calculated by the standby, then the standby goes for a reboot. From the next boot on-wards, the standby uses the indices stored in the DB for the session estimations. The previously mentioned procedure ensures that the indices and sessions estimates are same on the active and standby instances. **Workaround:** Run the following commands as root user on the active and standby instances. 1. The rm -f /opt/sonus/conf/swe /capacityEstimates/.indexMarker 2. Run a reboot
11	SBX-111363	2	The SBC VNF cannot get to Ready after a VNFM Migration. **Impact:** The VNF does not get ready after a migration to the new VNFM. **Root Cause:** When the new VNFM is trying to send the curl request to the VNF, the request is getting rejected. When the VNF gets deployed, it contains the VNFM data in its user data and it makes one VNFM IPs allowed list. This allowed list is not getting updated for the new VNFMs. So, when VNF migrates to the new VNFM, new VNFM IP is not present in the allowed list. **Steps to Replicate:** 1. Launch VNFM with https. 2. Deploy a VNF and scale out the VNFM. Migrate the VNF to the new VNFM. 3. The VNF state should be read and available.	The code is modified so whenever the new VNFM sends a request to VNF, it is accepted. **Workaround:** 1. 1. Reboot the setup. 2. 2. Add new VNFM IP in the /opt /sonus/conf/instanceLca.json before the application comes up. 3. 3. Check the state of the VNF on VNFM.

12	SBX-99253 | SBX-111358	2	SBX-99253: Customer ECGI to CA Mapping Enhancement. **Impact:** The SMM Switch operation is not working after an SBC reboot. **Root Cause:** The switchIndex is not being set properly during a config restore. **Steps to Replicate:** 1. Configure SMM Rule consisting of switch operation. 2. Run the Call. 3. Perform an SBC reboot. 4. Run the call (SMM will not be executed).	The code is modified to set correct the SwitchIndex during a config restore. **Workaround:** After a reboot, we can delete the SMM profile and configure again.
13	SBX-111339	2	CDR Viewer Download all button not working **Impact:** The CDR Viewer download all button was not working. **Root Cause:** An issue was caused when we changed the CSP. Due to that change, the content was made more strict and blob type were not allowed in Firefox and IE, resulting in a download failure. **Steps to Replicate:** 1. Log in to the EMA. 2. Navigate to CDR Viewer. 3. Select the Sip Ladder and click Download All. 4. Download is successful in Firefox/IE/Chrome.	The code is modified to allow the same to further processing. **Workaround:** No workaround.
14	SBX-110956 | SBX-111291	2	PortFix SBX-110956: Introduced the Upsampler for EVS in a EVS(wb)<=> NB codec scenario. **Impact:** The WB will not be used for EVS encoding and as a result, the channel aware mode cannot be enabled in an IDP NB scenario though negotiated through the SDP. **Root Cause:** There is an absence of an Upsampler in the Upstream path for EVS when WB is negotiated in an IDP NB scenario. **Steps to Replicate:** Run a EVS<=>G711 call with bw=wb; ch-aw-recv-5;br=5.9-13.2. In this case, the EVS encoder produces WB packets with channel aware mode enabled.	The code is modified for the EVS when the WB is negotiated in an IDP NB scenario. **Workaround:** None
15	SBX-109300 | SBX-111289	2	PortFix SBX-109300: The SBC should not accept cmr byte from discarded packets. **Impact:** The SBC was accepting the CMR from discarded packets. **Root Cause:** The CMR was being processed before Packet Validation. **Steps to Replicate:** Run and EVS<=>EVS call. Let the peer send 32Kbps packets having CMR for 24.4Kbps. In this case, the 32Kbps packets are discarded as we do not support transcoding beyond 24.4 Kbps for EVS. Also since the packets are discarded CMR for 24,4Kbps is also not honored.	The code is modified to validate the packet first followed by the CMR processing. **Workaround:** None.
16	SBX-109304 | SBX-111286	2	PortFix SBX-109304: The 13.2 wb cmr is not accepted when the SBC is operating in channel aware mode. **Impact:** The channel aware mode once enabled will always be enabled when the EVS encoder operates at 13.2Kbps and bandwidth WB. The only way to disable channel aware mode is to use a bitrate other than 13.2Kbps. **Root Cause:** The code to disable the channel aware mode if enabled on receiving on 13.2 WB CMR was absent. **Steps to Replicate:** Run a EVS to G711 call with br=13.2, ch-aw-recv-5; bw=wb. Stream a pcap having CMR for 13.2 WB from the peer. The call starts with 13.2 Kbps with Channel Aware mode being enabled. On receiving the CMR, the channel aware mode will be disabled while the bitrate is still 13.2.	The code is modified to address the issue. **Workaround:** None.
17	SBX-110439 | SBX-111280	2	PortFix SBX-110439: The DSP rejects CMR requesting channel-aware if localCodecMode is set to a value other than 13.2. **Impact:** The SBC was rejecting a Channel Aware Mode CMR when the current mode of operation of EVS encoder was not 13.2Kbps WB. **Root Cause:** A conditional check of the current Bandwidth and current Bitrate to honor a Channel Aware Mode CMR. **Steps to Replicate:** Run a EVS to AMRWB call with the following SDP: br=13.2-24.4; bw= nb-wb; ch-aw-recv=0 End point sends a CMR for Channel Aware Mode. In this case, the call starts with EVS encoder encoding packets as 24.4Kbps and on receiving the CMR, the rate changes to 13.2Kbps with Channel Aware mode enabled.	The code is modified to check if 13.2Kbps is a part of the activeCodecSet and whether WB is present in the bandwidth range negotiated to honor a Channel Aware Mode CMR. **Workaround:** None.

18	SBX-110299 | SBX-111278	2	PortFix SBX-110299 to 9.2 - MRFP does not active EVS partial redundancy mode during the call when the remote offers "ch-aw-recv=0" **Impact:** When the ch-aw-recv=0 is negotiated through the SDP, a CMR request for the Channel Aware mode with offset 2 and the priority HIGH was not being processed. **Root Cause:** The root cause of this issue was a wrong initialization of the channel aware mode offset and priority in the code. **Steps to Replicate:** 1. Run a EVS to G711 call with br=13.2; bw=wb;ch-aw-recv=0 2. Stream a pcap with CA CMR for priority HI and offset 2. Prior to the fix the CMR is not processed. With the fix, the CMR is processed and also honored.	The code is modified to address the issue. **Workaround:** None.
19	SBX-111270	2	The CDR record for DSP insertion/rejection reason field in 9.2.2R000 test execution has marked the call as “Transcoding” instead of “Transcoding due to DTMF”. **Impact:** The CDR DSP insertion reason is showing as trancoded instead of the DTMF for transcoded call with difference in DTMF parameters on the ingress and egress leg. **Root Cause:** The wrong code is present and overwrites the DSP insertion reason as transcoded. **Steps to Replicate:** Make a successful transcoded call with AMR codec on both sides and the DTMF parameter must be different in both ingress and egress.	The code is modified to set the DSP insertion reason based on the answered call leg. **Workaround:** None.
20	SBX-111256	2	The system level baseUdpPort is allowed to set higher than the range set at the IPTG level from the CLI. **Impact:** It is possible to set the system media mediaPortRange baseUdpPort value to a greater value than the value assigned to all the associated trunk groups, which is invalid. Example: set addressContext <name> zone <name> sipTrunkGroup <name> media mediaIpInterfaceGroupName <IPIG name>media mediaPortRange baseUdpPort 1030 set system media mediaPortRange baseUdpPort 1050 **Root Cause:** With the introduction of the SBC and realms, the validation code was incorrectly looking for realm data to validate the system level baseUdpPort against rather than the zone /address context/trunk group information that is used in SBC configurations. **Steps to Replicate:** Try to run the configuration below and check that an error report is now generated. commit Aborted: 'system media mediaPortRange': System base UDP port cannot be greater than mediaPortRange configured at a trunk group	The code is modified to correctly use the zone/address context/trunk group information to validate the baseUdpPort information on the SBC configuration. **Workaround:** Manually check the values on the trunk group before assigning the system level value.
21	SBX-111218	2	Invalid value for "45.20 Reason Header value Q850" in the ACT record. **Impact:** The invalid values populated in the CDR sub field 20 in ATTEMPT record. **Root Cause:** In the Signaling Application, during Call Failure the value passed to CAM module to populate in the CDR for the sub field bit 20 was out of Q850 range. This is due to not mapping the internal CPC cause code to the corresponding Q850 standard values. **Steps to Replicate:** Disable the Reason Header Q850 flag, and make a call. Reject the call with 607, where SIPTOCPC profile mapped as 607-216 post call release check the CDR Sub field - 20.	The code is modified to take care of mapping to right Q850 values. **Workaround:** None.
22	SBX-111177	2	The SBC inccorectly interprets RTCP packets as RTP when using DLRBT. **Impact:** The RBT (ring back tone) can be terminated early when the DLRBT (dynamic local ring back tone) is enabled and RTCP packets arrive with the B-party. **Root Cause:** When the DLRBT functionality was initiated it was not informed that RTCP could be received. This resulted in RTCP packets being treated as RTP and caused the SBC to think RTP was learned. As soon as SDP was received in 183, the SBC triggered cut through and the RBT was stopped even though the call was not answered. This left the A-party with silence until the call was answered. **Steps to Replicate:** Make a PSTN to MS Teams call with DLRBT enabled. Leave the call in ringing state with MS Teams for a long time and check that the ring tone is continually generated.	The code is modified to correctly identify RTCP packets and not use this as an indication to media being learned so that the ring tone continues to be played until real RTP packets arrive. **Workaround**: If RTCP is not required on the egress leg then disable it. If RTCP is required there is no work around.

23	SBX-111163	2	Export/import of the syslog configuration fails. **Impact:** The user-config-import command fails if the customer has configured the SBC to send the Linux level logs to a remote syslog server through the platformRsyslog configuration. **Root Cause:** The child configuration objects under the platformRsyslog configuration were not being applied in the correct order during the import, which led to the configuration validation logic thinking there was no syslog server configuration and failing. **Steps to Replicate:** Apply syslog configuration under the platformRsyslog and check that it can be exported and imported without errors.	The code is modified to correctly define the configuration order for platformRsyslog configuration so there are no errors during the import. **Workaround:** If you edit the syslogState line in the xml file and change it from enabled to disabled, the import will complete correctly. Then manually apply the CLI command to enable the syslogState once the rest of the configuration is imported. <platformRsyslog> <syslogState>disabled</syslogState> <linuxLogs> <platformAuditLog>enabled< /platformAuditLog> <consoleLog>enabled</consoleLog> <sftpLog>enabled</sftpLog> <kernLog>enabled</kernLog> <userLog>enabled</userLog> <daemonLog>enabled</daemonLog> <authLog>enabled</authLog> <syslogLog>enabled</syslogLog> <ntpLog>enabled</ntpLog> <cronLog>enabled</cronLog> </linuxLogs> <servers> <serverNo>server1</serverNo> <remoteHost>2607:f160:10:4043:ce:ff0:0:35</remoteHost> <protocolType>udp</protocolType> </servers> </platformRsyslog>
24	SBX-110984 | SBX-111144	2	PortFix SBX-110984: The EVS CMR not honored when in dtx period. **Impact:** If the SBC receives a CMR request when it is operating in DTX mode, the CMR was not being processed. **Root Cause:** The rate or bandwidth change received through a CMR was not put into effect after coming out of the no transmission period. **Steps to Replicate:** Run an EVS<=>EVS call with dtx enabled. On the Ingress leg, send a valid CMR while there is no media being sent on the Egress Leg. Send a CMR on the ingress leg when it is in the "no transmission period" Once the Ingress Leg comes out of the no tx period, the bitrate or the bandwidth as requested by the CMR should be put into effect	The code is modified to address the issue. **Workaround:** None.
25	SBX-111120	2	Customer Physical Server had a reboot failure. **Impact:** In a SBC Redundancy Group if an instance contains an SM core that did not cause service outage, the instance can go down when a switchover occurs between two other instances of same RG. **Root Cause:** The coreHandler/FacHandler process gets called to dump the core during a coredump on SBC if FAC feature is enabled. This process registered itself in sysIdList that is unintended and causes SM to crash while handling instance down event for other instances of same RG. **Steps to Replicate:** Create a RG, run it for few days and wait for an SM core due to the NTP, which does not cause the SBC to go down. Perform a switchover in same RG between two other nodes. The current node should not go down with fix build.	The code is modified to ensure the FacHandler does not register in sysIdList. **Workaround**: None.
26	SBX-110850 | SBX-111020	2	PortFix SBX-110850: Alter CPU Affinity of Processes in 2vcpu Scenario **Impact:** There are intermittent crashes of SWe_NP/SWe_UXPAD processes in 2 vcpu deployments. **Root Cause:** The SWe_NP and SWe_UXPAD DPDK processes running on the same core caused memory corruption in mempools. **Steps to Replicate:** 1. Bring up a 2 vcpu VM. 2. Run a heavy transcode call load for long duration.	The code is modified to launch the SWe_NP and SWe_UXPAD processes on different cores. **Workaround:** There is no workaround for this issue.

27	SBX-111004	2	The SCM Process cores on the customer PSBCs PS40, PS41, and PS42. **Impact:** A SCM Process coredump was observed because of Segmentation fault when a call was intercepted with PCSILI and media monitoring enabled. **Root Cause:** The SCM Process dumped core while pushing request for splitter resources and media monitoring was enabled. **Steps to Replicate:** 1. Configure the SBC and PSX for basic audio call. 2. Configure the customer CLI on Egress Leg for basic call. 3. Enable Media Monitoring on Egress leg for basic call. 4. Enable the Tones on Ingress Leg. 5. Perform an Interception based on PCSI_LI.	The code is modified to avoid the coredump. **Workaround:** None.
28	SBX-109211 | SBX-110945	2	PortFix SBX-109211: There was a design gap for AMR around dynamic codec transcoding. **Impact:** The SBC is configured with restricted AMR/AMR-WB codec in Egress Route PSP along with Transcode "If Different DTMF PT" enabled then consider Egress endpoint selects the first pass thru restricted AMR/AMRWB payload in Offer in its 200 O.K answer. In such a case, if the DTMF attribute of the payload doesn't match then the SBC will try to match the Answered AMR /AMR-WB codec with the transcode-able AMR/AMR-WB codec. In such a case the DTMF attribute will match but the mode-set match fails that causes a call failure. **Root Cause:**The SBC is configured with restricted AMR/AMR-WB codec in Egress Route PSP along with Transcode "If Different DTMF PT" enabled then consider Egress endpoint selects the first pass thru restricted AMR/AMRWB payload in Offer in its 200 O.K answer. In such a case, if the DTMF attribute of the payload doesn't match then the SBC will try to match the Answered AMR/AMR-WB codec with the transcode-able AMR/AMR-WB codec. In such a case the DTMF attribute will match but the mode-set match fails that causes a call failure. The partial matching of AMR/AMR-WB codec in a Offer Answer cycle was allowed early, and that was what caused the issue. **Steps to Replicate:** The SBC receives an INVITE with (AMR PT=96 and mode-set=1 and 2833 DTMF PT=101). Egress route is configured with AMR mode-set=0, 1, 2, 3, AMR PT=126 and DTMF PT=110 Egress route is configured to transcode for Difference in 2833 PT This causes the SBC to send out INVITE to UAS as follows: 96 (AMR mode-set=1) 126 (AMR mode-set=0,1,2,3) 110 (DTMF PT)	The code is modified so if the SBC transcodes the call due to Different DTMF, the transcoding is allowed and first offered payload type is used. **Workaround:** None.
29	SBX-110009 | SBX-110876	2	PortFix SBX-110009: The values in callsEstimate.txt differ between the Active and Standby SWe. **Impact:** The session capacity estimate values differ in active and standby VMs upon an LSWU upgrade of 1:1 the SWe HA pair. **Root Cause:** The following sequence of events resulted in the issue: 1. The processor indices are re-calculated upon LSWU upgrade, which differs from the processor indices calculated by the SBC VM in the earlier version. 2. The session estimates are calculated based on these new processor indices. 3. Post upgrade, once the application comes up, the processor indices that are stored in DB (from the older version VM), are restored back to the /opt/sonus/conf/swe /capacityEstimates/.index.txt file. As a result, the Active and Standby VMs obtained different session estimates upon upgrade. **Steps to Replicate:** After subjecting the 1:1 SWe HA to LSWU upgrade, content of the following file in Active and Standby VMs would differ: /opt/sonus/conf/swe/capacityEstimates/.callsEstimate.txt	The code is modified to retain the processor indices during the LSWU procedure. **Workaround:** After completing the LSWU upgrade, once the active(VM-A) and standby(VM-B) VMs are in sync, following a set of operations would make sure that session capacity estimates are identical in Active(VM-A) and Standby(VM-B) VMs: 1. Reboot the Standby (VM-B) VM. 2. The standby (VM-B) VM comes up with correct session estimates. Wait for the completion of application sync. 3. Now, reboot the Active(VM-A) VM. This results in application failover. Application running on the Standby (VM-B) VM takes over the active role. 4. Active(VM-A) VM comes up with the correct session estimates and comes in sync with the application running on the Standby(VM-B) VM.
30	SBX-105890 | SBX-110766	2	PortFix SBX-105890: On a disk failure, the correct failover is not triggered. **Impact:** On an SBC that was running 6.2 code, the disks on the SBC got into a bad state and would not process read or write operations. Automatic attempts to reboot the SBC from the application code failed and manual intervention was required to recover. **Root Cause:** Later software releases already had better handling for this sort of issue but the code was printing multiple logs as part of the automatic reboot process and it was suspected that these could have gotten hung and the system could not get to the reboot command. **Steps to Replicate:** The issue was not reproducible.	The code is modified to remove the logs to avoid the potential or not getting to actual reboot command in the code. **Workaround:** The SBC needs to be manually power cycled to recover.

31	SBX-109591 | SBX-110172	2	Portfix SBX-109591: Reject the INVITE with 100Rel when TG flag rel100Support is disabled and E2E Prack is disable on that leg after PSX DIP. **Impact:** The SBC does not tear down the call if the INVITE contains a Require: 100rel and the rel100Support flag is disabled on the ingress sipTrunkGroup, as per RFC3262. **Root Cause:** When the rel100Support flag is disabled and INVITE contains Require: 100rel, the SBC was not rejecting the Invite with 420 Bad extension. This scenario was not handled. **Steps to Replicate:** Set this flag: set addressContext default zone ZONE_IAD sipTrunkGroup TG_IAD signaling rel100Support disabled When the INVITE is received with Require: 100rel and endToEndPrack is disabled, the SBC should reject the call with a 420 Bad extension and the SBC should send header Unsupported: 100rel toward the ingress.	The code is modified so that when rel100Support flag is disabled and endToEndPrack is disabled. If the INVITE contains a Require: 100rel, the SBC will reject the INVITE with 420 Bad extension and the SBC will send header Unsupported :100rel toward the ingress. **Workaround:** None.
32	SBX-108410 | SBX-109379	2	PortFix SBX-108410: [ASAN]: sanitizer.CE_2N_Comp_ScmProcess_3.8866: ==CE_2N_Comp_ScmProcess_3==8866==ERROR: AddressSanitizer: heap-use-after-free on address 0x6190001c77dd at pc 0x558bcc9ff877 bp 0x7fea305f4e00 sp 0x7fea305f45b0 **Impact:** The ASAN reported a "AddressSanitizer: heap-use-after-free" error when a Subscribe request had a NULL character in a quoted string. ie: From: "00 test"<sip:user1@host> **Root Cause:** Invalid access of the freed memory occurred. Accessing memory after it is freed can cause unexpected behavior that may result in coredumps. **Steps to Replicate:** Run the codenomicon subscribe-notify suite.	The code is modified so the SBC now logs a parser error If the SBC receives NULL character in a quoted string. **Workaround**: None.
33	SBX-107798	2	The one way audio when forked leg is MS Teams without ICE/NAT. **Impact:** For an incoming call that is forked to multiple destinations and DLRBT is enabled, there is a possibility of audio flowing only in one direction when the call gets established. **Root Cause:** When a 180 ringing is first received from one of the forked destinations, this triggering the SBC to play ringback tone, but if the call subsequently receives 18x messages and RTP media (for media cut through) from a different destination, the SBC fails to activate the RTP media flow resources correctly at the ingress leg of the call because these resources are already activated for playing the ringback tone for the other fork. **Steps to Replicate:** Set up --------- The SBC configured with call forking such that call from ingress (A) to be forked to egress (B) and egress (C). The DLRBT should be enabled on ingress and egress trunk toneAndAnnouncementProfiles. Procedure ---------- 1. Initiate the call with an INVITE from A that should be forked to B and C. 2. From the egress endpoint B respond with 180 and then from egress endpoint C respond with 180. 3. From egress endpoint C respond with 183 with SDP. 4. Send the RTP media packets back from C to cause media CUTTHRU. 5. From egress endpoint C respond with 200 OK to connect the call. Expected Results ---------- 1. The INVITE sent to B and C. 2/3. The SBC sends back 180 towards A and starts to play ringback tone towards A. 4/5. The call is established, the SBC sends CANCEL towards B, ringback tone should stop and media should flow in both directions between A and C. Before the fix, media was not flowing from A to C.	The code is modified to re-activate the media resources after the call is answered on one of the forks and the remaining forks have been cleared. **Workaround:** Not available, but the issue does not occur if the DLRBT is not enabled.
34	SBX-106601	3	PortFix SBX-105609: Add a check for /boot parition free space in pre-checks. **Impact:** There was an upgrade failure due to insufficient disk space on /boot partition. **Root Cause:** There was an upgrade failed due to failure to copy the new boot images as part of upgrade due to insufficient disk space in /boot partition. **Steps to Replicate:** Upgrade to the fix build and ensure upgrade is successful.	The code is modified as part of pre-checks to ensure a minimum of 40MB free disk space is available on /boot partition. **Workaround**: None.

35	SBX-110292 | SBX-110789	3	PortFix SBX-110292: A Registration structure update is needed to prevent hijacking/hacking of the user after being rejected with a 403 Forbidden error. **Impact:** After a hack, the registers rejected with 403 Calls were not working. **Root Cause:** Both a normal and hacker user had very similar Register messages, except that the hacker's Auth header did not include the correct username. Due to this username mismatch, the SBC rejected the hacker with a 403 message, set the Register into 'challenged' state and later deleted the message. **Steps to Replicate:** There are 8 combinations of test cases. The major difference is in the username field Auth header. Test1: 1. Proper registration: Reg->401Reg (with Auth)200 2. Hacker registration: Reg->401Reg (with hacker Auth)403 3. Proper user refresh 4. Hacker registration: Reg->401Reg (with hacker Auth)403 Check for all fields and expiration timer. Test2: 1. Proper registration: Reg->401Reg (with Auth)200 2. Hacker registration: Reg->401Reg (with hacker Auth)403 3. Proper user refresh 4. Hacker registration: Reg (with hacker Auth)403 Test3: 1. Proper registration: Reg->401Reg (with Auth)200 2. Hacker registration: Reg (with hacker Auth)403 3. Proper user refresh 4. Hacker registration: Reg->401Reg (with hacker Auth)403 Test4: 1. Proper registration: Reg->401Reg (with Auth)200 2. Hacker registration: Reg (with hacker Auth)403 3. Proper user refresh 4. Hacker registration: Reg (with hacker Auth)403 Test5: 1. Proper registration: Reg (with Auth)200 2. Hacker registration: Reg->401Reg (with hacker Auth)403 3. Proper user refresh 4. Hacker registration: Reg->401Reg (with hacker Auth)403 Check for all fields and expiration timer. Test 6: 1. Proper registration: Reg (with Auth)200 2. Hacker registration: Reg->401Reg (with hacker Auth)403 3. Proper user refresh 4. Hacker registration: Reg (with hacker Auth)403 Test 7: 1. Proper registration: Reg (with Auth)200 2. Hacker registration: Reg (with hacker Auth)403 3. Proper user refresh 4. Hacker registration: Reg->401->Reg(with hacker Auth)403 Test 8: 1. Proper registration: Reg (with Auth)200 2. Hacker registration: Reg (with hacker Auth)403 3. Proper user refresh 4. Hacker registration: Reg (with hacker Auth)403	The code is modified so when the SBC rejects the hack because of a username mismatch in the Auth header, it reverts back to previous details and state (that is complete). **Workaround**: None.
36	SBX-103963 | SBX-107387	3	PortFix SBX-103963: Both SBCs restarted at the same time and both mounted drbd0. **Impact:** Both SBCs restarted at the same time and both mounted drbd0. **Root Cause:** The PRS Process was not updating the syncStatus flag value, due to which the the standby was also rebooting thinking the sync is not complete yet. **Steps to Replicate:** When both the the nodes are up and running, restart the standby. And while the standby is coming up, run a switchover from active CLI. The switchover should be successful.	The code is modified to use SMA API to check syncStatus instead of PRS and CHM local syncStatus flags. **Workaround**: None.

Resolved Issues in 09.02.02R000 Release

The following Severity 1 issues are resolved in this release:

Table 23: Severity 1 Resolved Issues

	Issue ID	Sev	Problem Description	Resolution
1	SBX-110842 | SBX-110869	1	PortFix SBX-110842: A switchover on the SBC 5000. **Impact:** The SAM process core dumped when the SIP code was attempting to lookup a internal SIP Registration Control Block. **Root Cause:** The core was the result of SIP code attempting to using a invalid index when accessing an array element for the purposes of finding a internal SIP Registration Control Block. **Steps to Replicate:** We have been unable to reproduce this issue. The root cause was found by code inspection and has been corrected.	The code is modified to prevent the use of an invalid index when accessing an array element. **Workaround:** There is no known workaround.
2	SBX-110833	1	There are call trace logging issues while all Call Trace filters are disabled. **Impact:** Messages traced at level 4 for sageTracing may erroneously have FILTER=<name> in the trace header. For the sageTracing, the filter name should be blank. With the sageTracing enabled, 70% of the received INVITES are traced at the level 4 and 0.5% of calls have all their messages traced at level 4. The sageTracing is tracing collected for the Strategic Analysis Gap Execution. **Root Cause:** The filter name messages traced for sageTracing should be blank but instead uses the 64th entry in the filter names table. **Steps to Replicate:** 1. The sageTracing is enabled. 2. Create at least 64 call trace filters and enable them. 3. Delete the trace filters. 4. Send INVITE messages.	The code is modified to filter the name blank. **Workaround:** None.
3	SBX-106871 | SBX-110165	1	Portfix SBX-106871: The SBC application times out while checking a callDetailStatus. **Impact:** The CLI 'show table global callCountStatus' timed out after a call setup failure due to the codec license not being available. **Root Cause:** The call setup failure in early stage caused an internal out of sync of the call resource, that triggers a handler of 'show table global callCountStatus' timeout when accessing the call resource. **Steps to Replicate:** Create a call in the SBC with no available codec license of the call.	The code is modified to clear the call resources in all related internal modules upon call failure in early stage to address the issue. **Workaround:** None.
4	SBX-100881 | SBX-109813	1	Portfix SBX-100881: The SBC sends a release to the H323 side. **Impact:** The SBC is sending a call release to the H323 side. **Root Cause:** During the codec selection on H323 side, the SBC ran into some offer-answer collision due to ACK SDP from SIP side. As a result, the SBC is terminating the call. **Steps to Replicate:** 1. Make a call from SIP to H323 and the call gets connected. 2. Send a late media Re-INV from SIP EP to the SBC. 3. The SBC sends 200 OK with SDP to SIP EP. 4. SIP EP sends ACK with SDP to the SBC. 5. The SBC sends a FACILITY to H323 EP. 6. The SBC terminates the call.	The code is modified so that the codec selection on the H323 side occurs independently during a modify offer-answer is in progress. **Workaround:** None
5	SBX-105657 | SBX-109924	1	PortFix SBX-105657: The Customer SBC Upgrade failed. **Impact:** The LSWU upgrade failed from 7.2.2R0 to 8.2.3R0. **Root Cause:** The /tmp partition was running out of disk space and the restoration failed during an upgrade. **Steps to Replicate:** Run a LSWU upgrade from 7.2.2R0 to 9.2.2.	The code is modified to ensure there is enough space available. **Workaround:** Free up some space in /tmp directory and re-run the upgrade.

6	SBX-110247 | SBX-110309	1	PortFix SBX-110247: The "sonusSbxNodePolicerMinorAlarmNotification" alarm is generated by the SBC. **Impact:** Packets arriving on a unallocated port do not get marked as rogue media. **Root Cause:** The issue occurs only on ports that was used and disabled. Packets arriving on this port get marked as grace-media packets. This is because a very high value of grace period is being incorrectly programmed for the udp port instead of the default 4 seconds. The high value is because of endianness. **Steps to Replicate:** 1. Reboot the VM. 2. Make a single normal call and wait for the call to end. Note down RTP UDP port of the SBC used in the call. 3. After the call has ended, stream UDP packets to the same RTP UDP port previously used in the SBC call. We will not see any u nallocated port rogue media entry for the stream. 4. Stream the UDP packets to a UDP port that has not been previously used in the SBC call. We will see rogue media entry for the stream.	The code is modified to perform the appropriate endianness translation on the affected fields to arrive at the correct value. **Workaround:** No workaround. This does not affect normal media processing, or associated statistics.
7	SBX-110323 | SBX-110823	1	PortFix SBX-110323: A SWe media Issue occurred after an active reboot **Impact:** Media issue after switchover. **Root Cause:** Before a switchover, the loopback call was set up with 2:xx:xx:x:x:x (vbsc1's pkt port mac address) for both src and dst MAC address. After switchover, from packet capture, we found that the SRC MAC address= 2:xx:xx:x:x:xx (vsbc2's pkt port mac address). As a result, using the srcMac and dstMac caused a media issue. **Steps to Replicate:** Use the following configurations to test: • Set up loopback and normal calls for both SBC HW and SWe platforms. • Do port and SBC switchovers. • Use single and alternate media IP addresses on the loopback ports.	The code is modified to use loopback flag mirrored to standby BRM, and overwrite both srcMac and dstMac if loopback flag is set to true. This is done only on SWe when enabling or modifying the RID. **Workaround:** No workaround.
8	SBX-109200 | SBX-110633	1	PortFix SBX-109200: Missing the CDR for Teams call transfer scenario. **Impact:** For an MS Teams blind transfer scenario with tonesAsAnnouncements enabled, where the MS Teams user A establishes a call to PSTN user B, then MS Teams user A establishes a call to user C and then invokes a blind transfer to establish the call between B and C. When the call is subsequently cleared one of the CDR STOP records for the call is not generated. **Root Cause:** When the tonesAsAnnouncements are enabled, after a blind transfer is initiated from user A, the subsequent call clearing logic is not correctly deactivating the internal announcement resources causing the call to not fully clear internally which results in STOP record not being generated. **Steps to Replicate:** With the SBC configured for MS Teams having DLRBT with announcementBasedTones enabled. Procedure ---------- 1. Establish a call from MS Teams User A to PSTN user B. 2. Establish a call from MS Teams user A to PSTN user C. 3. Initiate a blind transfer from MS Team user A, between user B and user C. 4. Clear the call and check CDR records. Expected Results ---------- Calls, transfers, and announcements should be successful. The SBC should generate START and STOP CDR records for A-B and A-C call.	The code is modified to correctly deallocate announcement resources for this call scenario so subsequent call clear can complete successfully and generate the correct CDR stop records. **Workaround:** If tonesAsAnnouncements are disabled the call scenario works as expected.

9	SBX-107976 | SBX-110218	1	Portfix SBX-107976: Disable the FAC feature in M-SBC, and SLB. **Impact:** Non-SIP SBC personalities should not have FAC feature enabled. **Root Cause:** Earlier, the SBC did not have personality check when setting core pattern. **Steps to Replicate:** Verify the user defined core pattern is not set in /proc/sys/kernel/core_pattern when instances are spawned with the personalities msbc,slb,mrfp irrespective of facState. %set system faultAvalancheControl facState <enabled/disabled> User Defined Pattern: cat /proc/sys/kernel/core_pattern |/opt/sonus/sbx/bin/CoreHandler -f /var/log/sonus/sbx/coredump/core.1.%e_%p.%t -t %i -p %p Default Core Pattern: cat /proc/sys/kernel/core_pattern /var/log/sonus/sbx/coredump/core.1.%e_%p.%t	The code is modified to not enable the user defined core pattern for personality type M-SBC, and SLB. **Workaround:** Disable the FAC Feature. %set system faultAvalancheControl facState disabled
10	SBX-107583 | SBX-108381	1	PortFix SBX-107583: There is one way audio on hairpinned calls. **Impact:** A one way audio problem is seen in a AMR-AMR transcoded call with DTMF interworking when "Different2833PTType" is enabled. This problem is visible for all HD codecs (AMR, AMR-WB, EVS, SILK) that uses dynamic payload in SDP offer. **Root Cause:** A one way audio problem is seen in a AMR-AMR transcoded call with DTMF interworking when "Different2833PTType" is enabled. This occurs because SBC incorrectly configures the DSP channel with an incorrect payload type, not the payload type which was negotiated during the Offer Answer exchange on the Egress leg. **Steps to Replicate:** 1. Enable "Different2833PTType" and TransCode conditional in PSP and set Preferred DTMF payload to 102 on both the PSP. 2. Send AMR payload 96,AMR-WB with DTMF 110 (8k) from Ingress. 3. Ensure Egress answer sends AMR 96 and DTMF 102 in answer. 4. Ensure that the call is transcoded and there is no way audio problem.	The code is modified so the SBC configures the DSP with pass thru payload type. **Workaround:** A code fix has been made.
11	SBX-107954 | SBX-110166	1	Portfix SBX-107954: The SBC CPXA coredump after EVS+T140 MRFP call. **Impact:** Occasionally, when the show global callDetailStatus command is executed in the CLI, the CPX process coredumps. **Root Cause:** If information is not available for a particular call, the data returned did not have a valid type for the Ip addresses returned. This caused a timeout out in confd because the CPX did not return information for the global callDetailStatus. **Steps to Replicate:** The steps cannot be reproduced.	1. The code is modified to return valid information for a call when information is not available. 2. The code is also modified to send a response to the CPX process when the application does not return proper data so that the CPX process will not crash. **Workaround:** Do not run the global callDetailStatus command.
12	SBX-108557 | SBX-109023	1	PortFix SBX-108557: The SBC continuously core dumps for SCM process since the upgrade to V09.02.01R000. **Impact:** ScmProcess may coredump due to memory corruption. **Root Cause:** There is code that is using an invalid pointer when writing to a buffer. This code was only added recently in 9.2.1R0. **Steps to Replicate:** This problem is triggered by the receipt of an invalid PDU and/or an SMM rule to reject the incoming Invite and an early ATTEMPT record was attempted to be written. The issue is random and depends on what info is NOT available when trying to write the accounting record, therefore the issue may not reproduce all the time.	The code that uses in invalid buffer pointer (which was added recently) has been removed. **Workaround:** If there is SMM rule (ignore/reject the Invite), then the SMM rule needs to be disabled until patch is applied.

13	SBX-108126 | SBX-108271	1	PortFix SBX-108126: Observed a SAM Process crash in another active node during SIPFE crash testing. **Impact:** The SAM Process coredumps due to a buffer overflow. **Root Cause:** The key:value length of incoming Message is max 255 bytes. But in the yang spec, the buffer length was defined as 23 bytes. As a result of this issue, the display was truncated and also crashing due to buffer overflow. **Steps to Replicate:** 1. Configure the testbed for the fault avalanche testing. 2. Trigger the crash by sending fac-sipfe-0 in the From header, where From(calling Party) is larger than 23 bytes. Expectation: 1. The current active should crash the SAM Process. 2. Standby will take over as active and blocks the SIP message that triggered crash.	The code is modified to handle 255 bytes string, so the buffer overflow does not happen and display is not truncated. **Workaround:** None.
14	SBX-108388 | SBX-108449	1	PortFix SBX-108388: The SBC set "user=phone" on Dummy History-Info header. **Impact:** When interworking between diversion header and history info header if the diversion count is more than 2 then the SBC generates dummy history info headers. These dummy history info headers contain user=phone which some end points reject. Example of a dummy history info header. History-Info: sip:unknown@unknown.invalid;cause=302;user=phone;index=1.1;mp=1 **Root Cause:** The code was mistakenly adding the user=phone attribute even when no phone number was present in the dummy history info header. **Steps to Replicate:** Configure the SBC to support interworking from diversion header with a count of 5 to history info headers and check that the dummy history info headers do not include user=phone.	The code is modified not to include user=phone in the dummy history info headers. **Workaround:** Use SMM to remove the user=phone attribute from the dummy history info headers.
15	SBX-109464 | SBX-109465	1	PortFix SBX-109464: Using a leadership algorithm workaround for an old openclovis issue can cause a core dump. **Impact:** Thesafplus_gms process crashes when coming out of split brain. **Root Cause:** There was incorrect/inconsistent data results in the code asserting. **Steps to Replicate:** This problem is not easily reproducible and is caused by HA link instability/flapping.	The code is modified so that the data is consistent. **Workaround:** The HA link stability.
16	SBX-109224 | SBX-110169	1	Portfix SBX-109224: AWS: The upgrade is failing with an error message " instance is not reachable " even though the upgrade status is "success :true" **Impact:** The AWS upgrade was failing due to instance non-reachability. In actuality, the VNFC was up and running but the VNFR showed VNFC status non-reachable. **Root Cause:** The VNFR-VNFC communicates using a ZMQ and VNFR updates the VNFC health check using the same ZMQ thread mechanism. There is a Zmqclient and ZmqServer. After an undetermined point in time, the VNFC(ZmqClient) is waiting for an infinite time to get a response from the VNFR(ZmqServer). This is leading to blocking state. **Steps to Replicate:** Run an upgrade/revert operations on 9.2.2/10.0.0.	The code is modified so the ZMQ communicates in non-blocking mode. **Workaround:** For the workaround, the user needs to run the pre check command from vnfr_intf before upgrade/revert operations and needs to take action provided as a part of output table.
17	SBX-109922 | SBX-110157	1	Portfix SBX-109922: The buffer used while printing PSP's was running out. As a result, this is an error. **Impact:** The buffer used while printing PSP's was running out because of large PSP. As a result, this is an error. **Root Cause:** The buffer used while printing PSP's was running out. As a result, this is an error. **Steps to Replicate:** 1. Run the suite with the RTCP Interworking Enhancements. 2. The warning above in the Opensaf logs should not come.	The code is modified to accommodate bigger strings. **Workaround:** None.

18	SBX-109336 | SBX-109925	1	Portfix SBX-109336: The SBC 5110: BIOS not updated to 2.07 post-upgrade as indicated in Release Notes. **Impact:** The BIOS is not upgrading part of the SBC application upgrade. **Root Cause:** The flashroom utility is using /dev and /proc file system to upgrade BIOS. these file systems are un-mounted part of grub2 config upgrade. **Steps to Replicate:** Upgrade the SBC app from 7.x (BIOS=2.6) to >= 8.1.x.(BIOS = 2.7). The BIOS should upgrade part of an application upgrade.	Mount /dev and /proc file system before calling BIOS upgrade **Workaround:** 1. Stop SBC App a. #sbxstop 2. Go to /opt/sonus/bios-update/ a. #cd /opt/sonus/bios-update/ 3. Run the script to update BIOS. a. # ./updateBIOS.sh bios5X00_v2.7.0-R0.rom This scripts will take few minutes to update BIOS, after its done reboot host. In next boot it will boot up with new BIOS.
19	SBX-108127 | SBX-110403	1	Portfix SBX-108127: 9.1r3 to 10.0 LSWU failed with the reason "Failed_to_install_or_configure_database" **Impact:** The LSWU failed with the reason "Failed_to_install_or_configure_database". **Root Cause:** Ownership for the files in /var/log/postgresql is getting changed at the time of the upgrade. **Steps to Replicate:** Perform an upgrade from any version to 9.x	The code is modified to restore ownership of the log files in /var/log /postgresql to postgress. **Workaround:** None.
20	SBX-108237 | SBX-108947	1	PortFix SBX-108237: Performance: Observed SAM and SCM process coredump for FAC enabled execution on SBC 5400 **Impact:** The SCM experiences a core dump when the Invite gets a transaction timeout and the 200 Ok for Invite is received at the same time. **Root Cause:** In the problem scenario, the SBC is trying to send ACK for the 200 OK, the SCM cores when creating a SIP Transaction for ACK Message. **Steps to Replicate:** 1. Run a Basic Invite call flow. 2. Do not answer for Invite on the UAS side. 3. After 32 seconds send 200 OK for Invite from the UAC side. A race condition might occur and result in coredump.	The code is modified not to send ACK in this scenario as the CseqType and CseNumber are unknown and 0 respectively. **Workaround:** Not Applicable.
21	SBX-107690 | SBX-108962	1	PortFix SBX-107690: There are SBC call failures observed on T140 load with various MAJOR logs in DBG. **Impact:** A call fails due to RID Enable errors. (where RID = receiver ID and is mapped to an allocated resource). ThenDBG log shows many BrmAsnycnCmdErrHdlr logs with cmd 0x30 (RID Enable): MAJOR .BRM: *BrmAsyncCmdErrHdlr: ERROR NpMediaIntf cmd 0x30 gcid 0x2128915e **Root Cause:** When the RTCP Generation is disabled, the RTCP RID for the call is expected to be disabled by Network Processor (NP). With the introduction of SBX-86241 "Streaming RTCP packets to Protect Server", we now have a case where RTCP Generation is enabled to stream RTCP packets to Protect Server but RTCP packets are not generated for the call and RTCP RID for the call is not enabled. When the RTCP Generation is disabled, the NP uses rtcpMode=RTCP Terminate to indicate that the RTCP RID needs to be disabled. This is incorrect since rtcpMode=RTCP Relay Monitor also has the RTCP RID enabled and NP is expected to disable the RTCP RID. If a call has the rtcpMode=RTCP Relay Monitor and RTCP Generation is disabled, we leak this particular RTCP RID resource. The next time, we try to allocate this particular RTCP RID, NP returns an error indicating RTCP RID is already allocated. **Steps to Replicate:** 1. Enable Packet Service Profile //Resources/profiles/media /packetServiceProfile/rtcpOptions /generateRtcpForT140IfNotReceivedFromOtherLeg. 2. On SBC, set //System/media/mediaRtcpControl /t140RtcpMonitorInterval to 20 seconds. 3. Start T140 call but do not send RTCP packet. Terminate call in 10 seconds. 4. If you keep making this type of call, you will eventually see the Enable RID error. DBG log will have the BrmAsynCmdErrHdlr entry.	The code is modified so the Bus Resource Manager (BRM) knows whether RTCP RID is allocated and needs to be disabled by NP. The code is also modified so that BRM indicates RTCP RID needs to be disabled or not. When NP receives the command, it uses this new parameter to decide if RTCP RID should be disabled or not. **Workaround:** Disable RTCP and disable RTCP termination.

22	SBX-109384 | SBX-110027	1	Portfix SBX-109384: The 8.2.4F001 SBC 5400 Global level SMM stopped to work. **Impact:** The Global SMM function stopped working post upgrade and similar issue was observed after multiple switchovers. **Root Cause:** The Global SMM configurations were not being restored. **Steps to Replicate:** 1. Attach an SMM at global level (for 200ok of pathcheck options). 2. Perform multiple switchovers or LSWU to another build. 3. Check if the SMM is being applied.	Restore the Global SMM configurations during multiple switchovers to address the issue. **Workaround:** Delete the profile set at global level and configure it again.
23	SBX-107430 | SBX-108140	1	PortFix SBX-107430: URI parameter setting order of R-URI does not meet RFC 3966 requirements. **Impact:** In the request URI, the isub parameter was after the NPDI parameter, which does not meet the RFC 3966 requirement. (ie. npdi; isub=1111) **Root Cause:** In the code (sipsgCallProcEngine.c), the isub parameter was getting populated after NPDI and other user parameter. **Steps to Replicate:** SipSgMapIsdnSubAddrToSipParam this function is responsible for populating isub parameter to request uri, this moved prior to all other parameter populating functions.	The code is modified so the isub parameter populating function is moved before all other parameter populating functions. **Workaround:** NA
24	SBX-108270 | SBX-110278	1	PortFix SBX-108270: The S-SBC sends a DNS SRV before completing all NAPTR query. **Impact:** The S-SBC sends DNS SRV before completing all NAPTR query. **Root Cause:** A DNS agent request timeout occurs after 10 seconds. Because the DNS agent sends the DNS lookup (NAPTR) request to DNS Client process, the DNS client process then queries to an external DNS server for NAPTR records. The DNS agent waits until 10 seconds then timeout's for each DNS lookup. As a result, the DNS request is failed with the first DNS server and query is still in process for a second DNS server. **Steps to Replicate:** Configure 2 DNS server's 1. Configure DNS global configuration to: admin@SBX136% show global servers DNS global retransmissionCount 14; retransmissionTimer 500; set addressContext default dnsGroup DNSGrp1 negativeDnsCacheSupport disabled 2. Configure dnslookupTimeoutTimer to 10 sec. 3. Stop the DNS server. 4. Make a call. Observation: 1. DNS should retransmit DNS NAPTR query to DNS server1 and after should move to DNS server2. 2. After 10 sec, NAPTR query shall stop. 3. The SBC should send SRV/A query to DNS Server2.	The code is modified to: 1. Add new configuration timer flag "dnslookupTimeoutTimer" for DNS lookup. 2. Once the lookup timer expires, the DNS client will stop sending same query to DNS server (Ex: if NAPTR query is re-transmitted towards the DNS server, after timer expire. NAPTR query will be stopped). **Workaround:** None.
25	SBX-107517 | SBX-108990	1	PortFix SBX-107517: Import configuration results in two different final status depending where you look at it. **Impact:** The postgres DB restore fails that leads to provisioning issues such as: The "show configuration" does not display a complete configuration related to policy entities like sipTrunkGroup, IpPeer etc. The "delete" operation fails for sipTrunkGroup and other policy related entities. The exportConfig does not contain policy related entitles. **Root Cause:** The PostgressDB restore is failing due to restricted permission. **Steps to Replicate:** Set up required: 1to1 S-SBC virtual platform and register it within Direct-Single type of cluster on EMS. 1. Configure 2 TG and saveAndActivate revision (e.g. revision 2). 2. Configure couple of more CLIs and save AndActivate (e.g revision 3). 3. Restore revision 2 either from CLI or EMS. 4. After restore is successful. try to delete a TG. Observed Application failure. After implementing the fix, use the 4 steps and as a result, the delete was successful.	The code is modified to permit an appropriate permission to postgres user while restoring the pg_policy dump. **Workaround:** Use the following steps: #cd /opt/sonus/sbx/scripts Update the oam-config.sh on active and standby the SBC as following: replace $CHMOD -R 660 $extractDir/ with $CHMOD -R 665 $extractDir/ accessRights=`$STAT -c %a $SONUS_TMP_DIR` $CHMOD 775 $SONUS_TMP_DIR find $RM -rf $extractDir and add following line below this $CHMOD $accessRights $SONUS_TMP_DIR Restore a revision that has pg_policy_xx.dump with correct Trunkgroup, ipPeer etc. entries.

26	SBX-110354 | SBX-110831	1	Portfix SBX-110354: After upgrading from V08.02 or V09.02 to 10.00.00R000 successfully, a REVERT from 10.00.00R000 to V08.02.04R000 is failing. **Impact:** Reverting from the higher software version to lower software version fails. **Root Cause:** The OAM does not upload restored revision against lower software version (ie. restore of config tar ball that was created on lower software version before upgrade). After following the MOP for downgrade when OAM comes up, it downloads the last revision uploaded on EMS (in this case config revision for higher software version). As a result, it fails to start the service because of a version mismatch. **Steps to Replicate:** 1. Spawn OAM + S-SBC on V08.02.04R000. 2. Create multiple revision (e.g revision 1, 2, 3, 4). 3. Upgrade to software version V10.00.00R000. The revision 5 gets created from revision 4, Create revision 6, 7, 8. 4. Restore to revision 4 -> revision 9 will get created and uploaded to EMS. 5. Downgrade to revision V08.02.04R000. Expected O/P: The OAM should come up with revision 10 created from revision 9.	The code is modified to upload a configuration when a revision that is created on a lower software version is restored. And after a downgrade, it picks the revision with software version where the downgrade is done. **Workaround:** None.
27	SBX-106475 | SBX-110899	1	Portfix SBX-106475: The Cloud SBC instances are not coming up after a fresh installation or rebuild and the MGMT I Pis unreachable in BLR-PC3. **Impact:** The SBC instances are not coming up after a fresh installation or rebuild and the mgmt ip is unreachable when using the X710 sriov vfs for pkt interfaces. **Root Cause:** The X710 driver reset has been known to experience a delay in completing, thus causing a cloud-init service failure. For example, after the OS boot (as part of renaming the interfaces by sonusdev), the X710 driver is restarted. When the X710 does not immediately reset, the next cloud-init service fails, and the system is not in proper state. **Steps to Replicate:** The SBC instances should come up properly after fresh installation or rebuild and mgmt ip should be reachable with all supported sriov vfs for pkt interfaces.	The code is modified so after the renaming is done and the network driver is restarted, wait for some seconds to check if all the nic ports are up and running in sonusdev itself, before exiting the service. This blocks all other dependent service from starting. Once the nic port are up, proceed with the system bring up. With these code changes, the nic does not come up then, we log it as critical log and expect the user to check on it. **Workaround:** None.
28	SBX-109597 | SBX-110158	1	Portfix SBX-109597: Observed SCM process crash on the newly active S-SBC during SWO testing. **Impact:** While the SBC is running in sensitive mode, observed the SCM Process core during a switchover testing under the 1000 cps call load. **Root Cause:** As part of switchover, all the connected calls are rebuilt on a newly active SBC. But, there may be a chance that the SBC can hold few stale entries related to active calls in the system, which will be cleaned up after some time. If any of these stale entries receive an unexpected events, that leads to a core dump. **Steps to Replicate:** 1. Run 1000 cps load with 120 CHT. 2. Perform a switchover by killing the PRS Process.	The code is modified to identify these events for the stale entries and ignore them to avoid a coredump when the SBC running in the sensitive mode. **Workaround:** None.
29	SBX-108225 | SBX-109351	1	PortFix SBX-108225: Observed core files on fresh installed VMware SWe. **Impact:** The SSREG and SLWRESD processes a coredump on VMware SWe due to the time being set in past. **Root Cause:** When the SBC is installed using ISO and then app is installed, the ntp sync is occurring while the application is running and in case the time is set in the past, it causes SSREQ and SLWRESD processes to core dump. **Steps to Replicate:** Launch with the NTP IP other than a default IP, check if a coredump occurs due to time being set in the past.	The code is modified to update the /etc/ntp.conf before the SBC comes up so the runntpdate can access the NTP server IP. **Workaround:** No workaround.

30	SBX-108219 | SBX-110162	1	Portfix SBX-108219: Observed a SAM Process coredump in SLB for 1000 cps Peering Call load. **Impact:** In a load run, there was a core being observed in the SLBDEBUG call when it hits the default states as part of the SBC message processing. **Root Cause:** In the SLB debug call, there was new line () being passed as part of a string. **Steps to Replicate:** Not reproducible. The issue seen once when running. Run 1000 cps INVITE call load with PRACK enabled.	The code is modified so the new line () is not part of the debug string. **Workaround:** There is no workaround identified for this issue.
31	SBX-110642 | SBX-110995	1	PortFix SBX-110642: A coredump occurs after a blind transfer call. **Impact:** The DNS process is coring when TEAMS blind transfer call is made. **Root Cause:** The NULLError check was missing before accessing DNS Group pointer in DNS module. This occurs when DNS Group is not attach to Zone. So get function for the DNS group pointer returns NULL. **Steps to Replicate:** PSTN to TEAMS TEAMS blind transfer to PSTN2 Expected Result: There should not be a coredump during the BT.	The code is modified so now the DNS group is fetched after setting the current DNS group to default DNS group, this is case when the DNS group IP not provided. **Workaround:** No workaround.
32	SBX-108612 | SBX-110161	1	Portfix SBX-108612: An SCM Process core dump occurred when INVITE with message size of 31700 bytes is sent **Impact:** Receipt of SIP messages with Content-Type: multipart/mixed and more than 10 content entries cause coredump, if a message manipulation rule is active with criterion on message body. **Root Cause:** Missing handling for unexpected message received. **Steps to Replicate:** 1. Configure and apply a message manipulation rule with criterion messageBody. 2. Send in INVITE with Content-Type: multipart/mixed and more than 10 content entries.	The code is modified so that if more than 10 content entries are present, the message is not considered for SMM rule actions with criterion on message body. **Workaround:** None.
33	SBX-109327 | SBX-111048	1	Portfix SBX-109327: Some CDR Events in ACT files have timestamps that are not current. **Impact:** Duration Field (+24 Duration of SIP Registration/Subscription Context) is not displayed for some register transaction. **Root Cause:** Duration Field (+24 Duration of SIP Registration /Subscription Context) is only updated in case of de-register for Successful transaction. **Steps to Replicate:** 1. Configure SBC for Registration/Subscription. 2. Perform following Registration. A ------REGISTRATION----->SBC-----REGISTRATION---->B A<--------404----------SBC<----------404----------B A ------REGISTRATION----->SBC-----REGISTRATION---->B A<--------200OK----------SBC<----------200OK----------B 3. Check CDR for "Duration Field" (+24 Duration of SIP Registration/Subscription Context)	The code is modified to display the duration of SIP Registration /Subscription context for every CDR event. **Workaround:** None.
34	SBX-106760 | SBX-107967	1	PortFix SBX-106760: Performance: While running IMS AKA Registrations on SWe KVM, cannot achieve 1000 subscribers with 30 RPS properly. **Impact:** The SBC was not able to achieve the IMS AKA registrations even at a lower rate (30 registrations per second). **Root Cause:** For one of the IPsec features, the XRM code was modified to perform route lookup and next hop destination MAC resolution during IPsec SA setup. This was causing a delay in setting up IPsec SAs during load causing timeouts during the IMS AKA registration. **Steps to Replicate:** Run the IMS AKA Registration load at 30rps.	The code is modified to not invoke the route loopup and destination MAC resolution code that is causing delay in setting up IPsec SA, which addresses the issue. **Workaround:** None.

35	SBX-110066 | SBX-110491	1	Portfix SBX-110066: Observed a SAM Process core dump in SLB while testing Performance with SLB (TLS Peering Calls) - One time Occurrence. **Impact:** A SAM Process core was observed on a shutdown. **Root Cause:** A race condition in the process shutdown code occurred allowing access to an invalid pointer, and causing a core dump during the shutdown of the SAM Process. **Steps to Replicate:** Restart the SBC and look for a SAM Process core.	The code is modified to avoid the race condition that led to the core. **Workaround:** No workaround, but since this core is during shutdown, there is no impact to normal operations of the SBX.
36	SBX-109953 | SBX-109984	1	PortFix SBX-109953: Performance: Observed NP_WRK0 Core on Active Instance on OpenStack while using VIRTIO. **Impact:** The SWe_NP can crash during a sbxrestart or sbxstop in the extra small memory profile. **Root Cause:** There is corruption due to incorrect use of global variable in an extra small memory profile. **Steps to Replicate:** 1. Bring up the SBC in extra small memory profile. 2. Run a sbxrestart or sbxstop.	The code is modified to address the issue. **Workaround:** None.
37	SBX-108310 | SBX-109287	1	PortFix SBX-108310: Various link monitor issues on the SBC SWEs with port redundancy enabled. **Impact:** On the VMware platform with Intel 82599 SR-IOV packet port VFs, the link does not get restored upon toggling the underlying physical link. **Root Cause:** Because of VMware PF driver shortcoming, DPDK ixgbevf PMD code does not get link up indication from link speed status register for SR-IOV VFs from Intel 82599 card. **Steps to Replicate:** 1. Bring up port redundancy setup on VMware with SR-IOV 82599 VFs packet port. 2. Toggle the carrier link state on the NIC by cable pull or interface link toggle on host through the IP commands. 3. Observe the link status is not restored.	The code is modified to detect the physical link loss from the NACK status set on the hardware mailbox register, specifically for the VMware platform. **Workaround:** No workaround. Only reboot clears the link state.
38	SBX-106858 | SBX-110390	1	Portfix SBX-106858: The SBC clears a call on receipt of 200OK answer - CFNA call. **Impact:** The SBC clears call on receipt of answer for a MRF transcoded call involving egress UPDATE followed by tone play. **Root Cause:** During tone play, the SBC detaches the MRF resource from the call since tone is played by SBC. However, the media endpoint resource facing MRF stays with the call that results in failure later while assigning MRF resource back to the call during answer processing. **Steps to Replicate:** The following events lead to failure in this call flow: 1. 183 with SDP from egress leads to cut-thru (MRF transcoded call). 2. Then, egress peer sends SIP UPDATE to the SBC. 3. Followed by 180 from egress which arms RTP monitoring at the SBC. 4. Followed by RTP failure notification after 2 seconds which starts Tone. 5. Followed by answer which results in failure.	Detach the media endpoint resource facing MRF from the call during tone play to address the issue. **Workaround:** None.
39	SBX-107492 | SBX-110168	1	Portfix SBX-107492: Observed a SCM Process core dump after 2 hours of load run with EVRCB to G711 transcode calls. **Impact:** During call load, the SIPFE module was crashing while writing date to a mapped address. **Root Cause:** The write to memory mapped address for files was causing a delay and leading to health check time outs causing core dumps **Steps to Replicate:** Run a 100 cps SIP-SIP call load for about 2-6hrs period of time.	The code is modified from file to Shared memory, which solved the problem **Workaround:** None.

40	SBX-110184 | SBX-110381	1	Portfix SBX-110184: Performance: While pumping Emergency call load on top of normal call load, HPC calls are getting rejected with 488 sip Error due to dsp overload even though resources were reserved on Openstack D-SBC HA. **Impact:** The HPC calls are rejected with 488 even though the SBC has sufficient DSP resources reserved for such calls through the highPriorityCompressionReservation configuration. **Root Cause:** In a D-SBC setup, when DSP allocation request is received, the T-SBC applies the call admission policy to know whether the call can be admitted or not before proceeding with DSP allocation. In this process, the T-SBC was not considering if the allocation request was for HPC call or normal call. As a result, the HPC calls were treated like normal call leading to rejections if this T-SBC is running under high load. **Steps to Replicate:** 1. Reserve DSPs for HPC calls. 2. Run a normal call transcoding at 200cps. 3. Run HPC transcoded calls at 5cps. 4. Ensure the HPC calls work as long as reserved DSP resources are not exhausted.	The code is modified to give preferential treatment to HPC calls during call admission policy at the T-SBC. **Workaround:** No workaround.
41	SBX-107137	1	A DEADLOCK was detected for sysID 85, task CHM. **Impact:** Health check timeout resulted in deadlock for CHM and process crash to recover. **Root Cause:** The CDB read call took longer than a health check interval resulting in CHM process being crashed to recover. **Steps to Replicate:** The problem could not be reproduced.	The code is modified so the health check timeout is increased to 30 now from previous 10. The longer health check interval allows for unexpected cases where processing can take longer than expected especially on SWe systems. **Workaround:** None.

42	SBX-110303	1	The MGMT Port Status was showing the wrong status. **Impact:** An Unconfigured Management port is shown as UP when there is no cable connected to the port. **Root Cause:** The SBC did not keep track of management port status if the management port is not configured/used. **Steps to Replicate:** 1. Show the issue. a. Leave SBC 5400 mgt2 port unconnected. b. Display mgmtPortStatus - the unconnected mgt2 shown as admnEnabledPortUp. This is the issue. admin@YF01> show table system ethernetPort mgmtPortStatus CE PORT IF NEGOTIATED DUPLEX RX ACTUAL TX ACTUAL RX TX RX NAME NAME INDEX MAC ADDRESS SPEED LINK STATE MODE BANDWIDTH BANDWIDTH PACKETS PACKETS ER --- YF01 mgt0 1 0:10:6b:3:c8:d speed1000Mbps admnEnabledPortUp full 232 0 45 3 0 YF01 mgt1 2 0:10:6b:3:c8:e speed1000Mbps admnEnabledPortUp full 0 0 6 2 0 YF01 mgt2 3 0:10:6b:3:c8:f unknown admnEnabledPortUp unknown 0 0 0 0 0 YF01 mgt3 4 0:10:6b:3:c8:10 speed1000Mbps admnEnabledPortUp full 0 142 2 42 0 [ok][2021-05-18 10:32:15] 2. Show the fix. a. Leave SBC 5400 mgt2 port unconnected. b. Display mgmtPortStatus - the unconnected mgt2 shown as admnEnabledPortDown (this is the fix). admin@YF01> show table system ethernetPort mgmtPortStatus CE PORT IF NEGOTIATED DUPLEX RX ACTUAL TX ACTUAL RX TX NAME NAME INDEX MAC ADDRESS SPEED LINK STATE MODE BANDWIDTH BANDWIDTH PACKETS PACKETS --- YF01 mgt0 1 0:10:6b:3:c8:d speed1000Mbps admnEnabledPortUp full 248 0 271 6 YF01 mgt1 2 0:10:6b:3:c8:e speed1000Mbps admnEnabledPortUp full 0 286 27 103 YF01 mgt2 3 0:10:6b:3:c8:f unknown admnEnabledPortDown unknown 0 0 0 0 YF01 mgt3 4 0:10:6b:3:c8:10 speed1000Mbps admnEnabledPortUp full 0 0 0 8 [ok][2021-05-18 13:32:27] admin@YF01> c. Display alarms and make sure there is no alarm on mgt2 (un-configured management port) admin@YF01> show table alarms currentStatus ALARM CLEAR ID TYPE TIMESTAMP INITIAL TIMESTAMP COUNT DESC --- 1237 AUTOMATIC 2021-05-18T17:27:53-00:00 2021-05-18T17:27:53-00:00 1 System Policer Alarm Level: Minor, Policer [ok][2021-05-18 13:32:30] admin@YF01>	Keep track of the management port state changes even if there is no Management IP interfaces on the management ports. Do not generate management port down event if there is no Management IP interfaces on the management port. **Workaround:** None. Optionally, connect unused management ports to Ethernet switch to reflect the port UP status.
43	SBX-109893	1	The SBC frequently performs a switchover with a core dump after a 9.2.1R0 upgrade. **Impact:** An SCM experienced a core dump in the code that is executed only when the STI feature is enabled. The core dump was the result of code in SipSgStiCopyDisplayNametoCPC() attempting to de-reference a NULL pointer. The fix is to add a check for NULL before attempting de-reference the pointer. **Root Cause:** The root cause is that there is code in an STI specific function that attempted to de-reference a NULL pointer. A NULL pointer check is missing in this code. **Steps to Replicate:** Specific steps to reproduce this issue are not known. The root cause and the fix were found through code inspection and core analysis.	The code is modified to add a check for NULL before attempting de-reference the pointer. **Workaround:** The only known workaround is to disable STI.

44	SBX-109055	1	Error in EMA when modifying and saving sipAdapterProfile. **Impact:** Error in EMA when modifying and saving sipAdapterProfile. **Root Cause:** The scenario comes up when profile name has ellipses in datatable. If profile name is very big, ellipses (...) will be added at the end, due to this the actual profile name is not passed back during save operation. **Steps to Replicate:** 1. Login in to EMA. 2. Navigate to SIP Adaptor Profile. 3. Select the profile that has ellipses (..) and modify then save it. 4. Profile gets saved with any error.	The code is modified to match if ellipses present in profile name, getting the title of selected entry from datatable. The title is not available in profile name without ellipses thus taking text from selected entry. **Workaround:** No workaround.
45	SBX-110003	1	There was a SBC 5400 core dump after MSRP call with direct media. **Impact:** A PRS core was encountered when customer was running MSRP with direct media and MSRP Multiplexing was enabled. **Root Cause:** The root cause is that the MRM code is using an invalid index to get a pointer to an array element. **Steps to Replicate:** This is not reproducible as it is most likely triggered by a race condition.	The code is modified the ensure that MRM uses the correct index when attempting to get a pointer to an array element. **Workaround:** The only known workaround is to avoid running MSRP with direct media and MSRP Multiplexing.
46	SBX-107983	1	The LSWU from V07.02.00-R002 to V09.02.00-R001 has failed with the error "CpxIntfErrorExit". **Impact:** Upgrade fails and the SBC fails to come up due to missing SNMP configuration. **Root Cause:** The targetAddrsParams for standard V2 trap had been removed from the configuration and this information was expected to be present during the upgrade processing. **Steps to Replicate:** Perform upgrade with SNMP configuration in place and check for errors in the CE_Node.log file.	The code is modified to identify the SNMP upgrade failures. **Workaround:** Manually add back in targetAddrsParams for traps.
47	SBX-110059	1	The SBC upgrade failed as the SNMP trapTarget with a name containing white-space. **Impact:** If any SNMP trapTarget name contains a space, upgrade to 9.2.1 will fail. **Root Cause:** A trap target is configured with a name containing a space character, which is allowed for this table. **Steps to Replicate:** On 8.2 software, use CLI to create a trapTarget with space character: set oam snmp trapTarget "test target" ipAddress 1.2.3.4 state enabled Perform an upgrade to 9.2.1.	The code is modified so that it can cope with trapTarget names with space characters. **Workaround:** Prior to upgrade ensure no trapTarget names have space, recreate with a new name not containing space.
48	SBX-109174	1	The SBC unable to load config after upgrading from 7.2.3S400 to 10.0 A006 **Impact:** After upgrading a cloud SBC from a pre 9.2.0 version, unable to reload the config when the 'SystemName' is not set to 'vsbcSystem' **Root Cause:** The configuration filename pre 9.2.0 uses 'vsbcSystem' instead the of the defined 'System Name', meaning the SBC is unable to find the file to load it. **Steps to Replicate:** 1. Save a configuration on a cloud SBC pre 9.2.0 (e.g. AWS). 2. Upgrade the SBC. 3. Attempt to load the configuration file.	The code is modified to address the issue. **Workaround:** Change configuration filename to be that of the set 'SystemName'. e.g. If 'SystemName' is set as 'aws-sbc' change: config_vsbcSystem_20210414_035150.tar.gz -> config_aws-sbc_20210414_035150.tar.gz

49	SBX-110639 | SBX-111102	1	PortFix SBX-110639: When the call is dipped the invite sends only the LRN. **Impact:** When ingress INVITE's DIVERSION header does not present and TO header is different from RURI, i.e., it has redirecting original number, the egress RURI will take translated number, i.e., LRN, as RURI in egress INVITE, after LNP dip. **Root Cause:** The RURI should take LRN in egress, while DIVERSION header in ingress presents. But the code change for a previous issue has made RURI equal to LRN even DIVERSION header was missing. **Steps to Replicate:** 1. Set up SIP to SIP LNP call, on SBC and external PSX system. 2. The TO header username (phone number) is different from RURI. 3. There is no DIVERSION header. This should reproduce the problem and test the fix. Please go through all regression test related to SBX-106067. It's important NOT to break any functionalities in SBX-106067.	The code is modified the condition to only set RURI equal to LRN while DIVERSION header presents. **Workaround**: None.

The following Severity 2-3 issues are resolved in this release:

Table 24: Severity 2-3 Resolved Issues

	Issue ID	Sev	Problem Description	Resolution
1	SBX-104733 | SBX-110295	2	Portfix SBX-104733: SCM Process core dump during healthcheck. **Impact:** The SCM Process core dumped when too many set operations executed in a single commit. **Root Cause:** The Call Processing tasks takes longer than 10 seconds when subscribing to the changes made to SIP Trunk Group. **Steps to Replicate:** Configure 12 trunk groups. Modify 11 trunk groups with a single commit command and the CLI will deliver the following error message: Aborted: 'addressContext default zone ZONE_IAD sipTrunkGroup': Too many set operations between commits. Revert the session and retry(max set operations 10). Again modify 10 TG in single commit: O/P: commit complete	The code is modified per commit is changed to 10 from earlier value of 50. **Workaround:** Ribbon recommends performing a commit after every CLI transaction.
2	SBX-104619 | SBX-109911	2	PortFix SBX-104619: The FM process coredumped. **Impact:** The FM Process crashed and wrote coredump. **Root Cause:** The FM Process tried to read the /proc/meminfo file, which should always exist, but it got a file not found error. **Steps to Replicate:** It is not known how to reproduce this as this should never happen, so defensive code added to prevent null read/write.	The code is modified so when we cannot read the /proc /meminfo file, we return the last good value read instead of a NULL to prevent the crash. **Workaround:** None.
3	SBX-109177 | SBX-109282	2	Portfix SBX-109177: The SbcSftp throws an error as "Failed to add ACL". **Impact:** The sbcsftp application does not remove the ACL created correctly. **Root Cause:** The permissions to delete the ACL gets lost while lowering permissions to ensure the sbcsftp can only access the current user's files. **Steps to Replicate:** 1. Run SbcSftp as linuxadmin. Verify no 'Failed setting permissions' error messages appear. 2. Verify Cleanup Script: a. Run SbcSftp but kill the the process before it completes, with 'kill -9 $PID'. b. As root, get the name of the ACL: '$CPSI -d acl | grep SbcSftp'. c. Wait 15 minutes. d. Verify ACL removed: '$CPSI -d acl | grep SbcSftp'.	The code is modified so that we can raise the permissions again once SFTP is complete. **Workaround:** None.

4	SBX-109968 | SBX-110233	2	PortFix SBX-109968: The 822R0 SCM Process core dumped. **Impact:** The SCMProcess core dumped on a SWe. **Root Cause:** Active SCM sent a Redundancy message to Standby SCM with a Registration index that was outside of its MAX range. The error handling code caught this and attempted to clean up the Registration Control Block but had a problem because the Control Block had not yet been initialized. **Steps to Replicate:** This problem is not reproducible. It is most likely triggered by a race condition which results in the Active and Standby to have different numbers for max number of Registrations (on a SWe the max number of Registrations comes from the file callEstimates.txt and in this case, the files on the active and standby do not match). This appears to be a SWe specific issue (the callEstimates.txt file is only used in SWE setups).	The code is modified to initialize the Registration Control Block immediately after allocating it, before any validation checks, so that the error handling code can clean up the RCB without causing a core. **Workaround:** There is no known workaround.
5	SBX-110215 | SBX-110387	2	Portfix SBX-110215: A coverity issue. **Impact:** Code fix for an SCM coredump (SBC-108237) when the Invite gets a transaction timeout and the 200 Ok for Invite is received at the same time needed some cleanup. Coverity issue: CID:338630 **Root Cause:** In the problem scenario, the SBC is trying to send ACK for the 200 OK, when the SCM cores while creating a SIP Transaction for ACK Message. **Steps to Replicate:** 1. Run a Basic Invite call flow. 2. Do not answer for Invite on the UAS side. 3. After 32 seconds, send 200 OK for Invite from the UAC side. A race condition might occur and result in coredump.	The code is modified not to send ACK in this scenario as the CseqType and CseNumber are unknown and 0 respectively. **Workaround:** None.
6	SBX-101432 | SBX-109029	3	PortFix SBX-101432: Question about the DSP insertion. **Impact:** Customer was seeing the "DSP insertion/rejection reason" CDR fields set to "Rejected codec unlicensed" and wanted to know why. **Root Cause:** The documentation did not provide any guidance as to when this value could appear. **Steps to Replicate:** The customer call scenario is unknown.	The code is modified to provide guidance on when it could happen as per the scenario below: These are the cases when DSP Rejection reason can be set to "Rejected codec unlicensed" 1. The SBC does not have a DSP. 2. The SBC has DSP but codec licenses absent. 3. The SBC has DSP and codec licenses but transcoding not enabled for the codecs. In any of the above cases if passthrough is possible and if the call is successful then DSP Rejection reason updates after a successful offer answer. This value might appear in the case where the offer /answer exchange did not complete. As the customer was unable to provide details on the specific call flow additional info level logging and call trace logs is modified as well to provide more details for the future. **Workaround:** None.
7	SBX-108143 | SBX-110227	2	Portfix SBX-108143: Set FAC as enabled by default. **Impact:** The FAC was enabled by default in 9.2 but was disabled in release 9.2.1. It is now enabled by default in further releases of 9.2.x and 10.0. **Root Cause:** The FAC was temporarily disabled by default until performance issues were fixed. **Steps to Replicate:** Run the FAC impacts performance on high cps, and perform load test.	The code is modified so the shared memory is used instead of memory mapped files. **Workaround:** Keep the FAC disabled if using high cps until it is upgraded to fixed version.
8	SBX-101239 | SBX-110571	2	PortFix SBX-101239: The congestion seen in a SBC with no traffic. **Impact:** The SBC 5400 reporting congestion even when no calls active. **Root Cause:** On the 5400 server, the EMA has allocated 4 CPUs for java and there are times when these can all run hot even when no calls on the system. The minimum number of hot CPUs to trigger congestion on the 5400 was set to 4 so it could report without any calls. **Steps to Replicate:** Enable SIP ladder diagram and CDR viewer on check for congestion reports on an idle system.	The code is modified to avoid congestion when no calls. This is similar to the other 5xxx models where the hot CPUs is one more than the number of java CPUs in EMA. **Workaround:** Disable SIP ladder diagram and CDR viewer services to reduce the java CPU usage.

9	SBX-105436 | SBX-109736	2	Portfix SBX-105436: The CDR issues for REGISTER. **Impact:** There were issues while writing CDRs for REGISTER method. **Root Cause:** The issues below were present w.r.t REGISTER CDRs: 1. CDRs were not generated for REGISTER in case of crankback scenarios. 2. TG name was not updated properly for REGISTER CDRs. 3. Disconnect reason was not updated properly for REGISTER CDRs. **Steps to Replicate:** 1. REGISTER an endpoint through SBC with/without crankback. 2. Check CDRs. Entries should be proper.	The code is modified for: 1. Generating EVENT records for REGISTER in case of crankback scenarios. 2. Correcting the egress TG name in the EVENT CDR for REGISTER. 3. Correcting the disconnect reason in the EVENT CDR for REGISTER. **Workaround:** None.
10	SBX-108198 | SBX-110388	2	Portfix SBX-108198: Coverity issues in nrsPktLifCsv.c **Impact:** There was a coverity fix that caused the issue. **Root Cause:** Fix added for the Coverity error. **Steps to Replicate:** The issue cannot be reproduced.	The code is modified to address the issue. **Workaround:** None.
11	SBX-108058 | SBX-110927	2	Portfix SBX-108058: The SBC CpxAppProc memory leak. **Impact:** During the SBC startup processing there is a small memory leak. **Root Cause:** During the startup processing, the SBC is allocating memory while reading configuration information and it is not being freed up correctly at the end of the provisioning steps. **Steps to Replicate:** This issue was only observed while running with ASAN images in the engineering lab as the amount of memory leaked is small and cannot be checked.	The code is modified to correctly free the memory allocated while processing the configuration data. **Workaround:** None.
12	SBX-105856 | SBX-110160	2	Portfix SBX-105856: The Wrong Version in URL after a Restore to an older version. **Impact:** The wrong version in URL after a Restore to an older version. **Root Cause:** URL is picked from CDB from path "/system/objectStoreParameters /url" that is independent of software version of revision. **Steps to Replicate:** 1. Spawn OAM act, standby and one SSBC with V10.00.00A008. 2. Create multiple revisions (e.g., rev1, 2, 3, 4, 5) 3. Upgrade cluster to V10.00.00A009. [root@VSBCSYSTEM-2-vsbc2 172.12.34.567 evlog]# cat /mnt/gfsvol1 /config-versions.txt 5,V10.00.00A008,oam_config_20210510T042937.tar.gz,0,2021-05-10T04: 29:37,,downloaded_from_ems 6,V10.00.00A009,oam_config_20210510T043100.tar.gz,1,2021-05-10T04: 31:00,REBOOT_REQ,auto_save_after_software_change [root@VSBCSYSTEM-2-vsbc2 172.12.34.567 evlog]# 4. Manually reboot and replace the SM Process with a fix. 5. Restore revision 3. 7,V10.00.00A008,oam_config_20210510T045034.tar.gz,6,2021-05-10T04: 50:34,RESTORE,restored_from_3 8,V10.00.00A009,oam_config_20210510T045311.tar.gz,6,2021-05-10T04: 53:11,REBOOT_REQ,auto_save_after_software_change Observation: Revision 7 uploaded with correct URL. 6. Remove revision 7 from /mnt/gfsvol1 and restore revision 7. Revision successful and newly created revision uploaded on EMS with correct URL 11,V10.00.00A008,oam_config_20210510T055545.tar.gz,20,2021-05-10T05:55:45,RESTORE,restored_from_9 12,V10.00.00A009,oam_config_20210510T055745.tar.gz,20,2021-05-10T05:57:45,REBOOT_REQ,auto_save_after_software_change	The code is modified to update the URL with software version of revision being restored. **Workaround:** None.
13	SBX-108356 | SBX-110006	2	PortFix SBX-108356: The SBC has various runtime errors found in np.log. **Impact:** Internal ASAN builds report runtime errors on SWe platform related to left shift of signed integers. **Root Cause:** Appropriate integer casts were missing in code, which caused ASAN runtime warnings related to bit shift. **Steps to Replicate:** Bring up ASAN build on SWe platform and observe if np.log contains ASAN runtime warnings related to bit shifts.	The code is modified to fix the runtime warnings in ASAN builds. **Workaround:** No workaround.

14	SBX-102925 | SBX-110143	2	Portfix SBX-102925: The issues in Ova\QCow2 installation **Impact:** The SBC SWe installed through the ISO and SBC SWe created through the image launch method have different prompts and root password. **Root Cause:** While installing through the image launch method, the SBC SWe was getting configured the cloud SBC way w.r.t root password and prompt. **Steps to Replicate:** 1. Install the SBC SWe using the ISO. Check the root password and CLI prompt. 2. Instantiate the SBC SWe using Image launch. Check root password and CLI prompt. Results from step 1 and step 2 should be same.	The code is modified to ensure both image launch method and ISO install method of the SBC SWe has no root password and same CLI prompt. **Workaround:** The user can manually remove root password on ISO installed SWEs using below command: usermod root -p '*'
15	SBX-110179 | SBX-110217	2	Portfix SBX-110179: The LeakSanitizer: detected memory leaks. **Impact:** A memory leak occurs when a logical management interface is added or modified. **Root Cause:** A confd cursor element was not closed when exiting the routine that validates the logical management interface being added or changed and this resulted in a memory leak. **Steps to Replicate:** Make changes to the logical management interfaces and check for memory increasing in the Cpx process.	The code is modified to ensure the associated memory is freed to avoid the leak. **Workaround:** None.
16	SBX-105763 | SBX-110036	2	PortFix SBX-105763: Move the dmesg monitoring from SM to a platform cron job **Impact:** Move dmesg monitoring from SM to a platform cronjob **Root Cause:** Since the dmseg can be large for long-running SBCs (thus, take longer to dump logs), the function can take longer causing an SM healthcheck. **Steps to Replicate:** Check for "/var/log/sonus/tmp/dmesgErrorMarker.tmp" after manually running the script	The code is modified to run every minute as a cron job to find i/o and filesystem errors in dmesg. If error is found, it'll create a marker file in tmp, which can be later used by other script to check sanity of the system. **Workaround:** None
17	SBX-94852 | SBX-110154	2	Portfix SBX-94852: Security, Audit and other logs modifiable (including deletion). **Impact:** Administrator users are able to delete or modify evlog files on the SBC. **Root Cause:** Users belonging to upload group(like admin) had write access on the evlog dir, which allows them to delete/modify log files. **Steps to Replicate:** Use SFTP to login to the evlog directory as user admin, and attempt to modify/delete log files.	The code is modified that prevents the admin from having writing access on the files owned by other users. **Workaround:** None.
18	SBX-108435 | SBX-109815	2	Portfix SBX-108435: The SBC CpxApp Process dumps core in the standby OAM. **Impact:** The CPX coredump occasionally writes when the SBC is stopped. **Root Cause:** Replication Engine thread is not stopped when the CPX receives deactivate request. **Steps to Replicate:** It is rarely reproducible.	The code is modified to address the issue. **Workaround:** None.
19	SBX-106543 | SBX-110144	2	Portfix SBX-106543: The SBC experiences a core dump while running UAS Notify Request. **Impact:** The SBC coredumps while processing the UAS Notify Request within the XML body. **Root Cause:** In API SipsCheckForAnyBody(), the loop where the string pointer pch is incremented each time was being accessed before validating for an out of bounds condition that caused the crash. **Steps to Replicate:** Send a NOTIFY with XML body from UAC towards the SBC.	The code is modified to add a out of bounds check before accessing the pointer value. **Workaround:** None.
20	SBX-108370 | SBX-110816	2	Portfix SBX-108370: The top2 on the SBC core takes lot of CPU cycles. **Impact:** The SBC performance monitoring tools like top2 at times take 20% of a CPU core there by reducing total available CPU resources for management activities on SBC. **Root Cause:** Introduced nice values to sbxPerf commands but still top2 taking around 20-30% at times. As a result, need to check ways to optimize it to take less CPU using /root/.top2rc. **Steps to Replicate:** Install fix build and by using top command make sure CPU utilization of top2 should not be much CPU utilized.	The code is modified to take less CPU utilization of the SBC performance monitoring tools like top2. **Workaround:** None.

21	SBX-109681 | SBX-110923	2	Portfix SBX-109681: Low MOS score for UNENCRYPTED_SRTP calls **Impact:** In SRTP for unencrypted, Authenticated case, SRTP packets were being discard at NP due to authentication key mismatch. **Root Cause:** In SRTP for unencrypted, authenticated combinations key size is required in NP to derive the session authentication keys. Since the cipher key size was not being pass to NP, session authentication key was wrongly calculated. **Steps to Replicate:** On the receipt of an SDP offer with crypto attributes, if 'enable SRTP' is Configured in packet service profile, a common crypto suite is found in the crypto attribute received in the offer and in the packet service profile, and session parameters if included are allowed, the offer will be accepted. In the answer, the SBC includes the same tag used in the offer. Test Setup on the SBC: 1. Endpoint1 Configured with SRTP profile(SRTP/SHA-1-80). Disable all Session Parameters in packet service profile. Allow Fallback enabled. 2. Endpoint2 Configured with SRTP profile(SRTP/SHA-1-80).Enable Session Parameters UNENCRYPTED_SRTP in packet service profile. Allow Fallback enabled. Procedure: Endpoint1 sends an offer SDP with crypto attribute SRTP/SHA-1-80 and with Session Parameters UNENCRYPTED_SRTP Endpoint2 replies with crypto attribute SRTP/SHA-1-80 and with Session Parameters UNENCRYPTED_SRTP	The code is modified so the SBC application is passing cipher key size also to NP to calculate session authentication keys. **Workaround:** Workaround is to not send unencrypted SRTP. Use cases with Encrypted SRTP and authentication no issue is seen.
22	SBX-105900 | SBX-110229	2	Portfix SBX-105900: Resize log volume on every boot. **Impact:** The log volume is not being resized on every boot. **Root Cause:** Currently, we build the filesystem on cinder volume only on the first boot. **Steps to Replicate:** 1. Create and attached a cinder volume of 50 GB. 2. Bring down the SBC, resized cinder volume to 100 GB. 3. Launch the SBC with the cinder volume attached. Check if the cinder volume is resized to 100 GB.	Check if file system is already built. If the file system is not built, resize the volume to address the issue. **Workaround:** None.
23	SBX-108190 | SBX-110223	2	Portfix SBX-108190: SBC: The callTracing does not work after reverting a switchover. **Impact:** You cannot enable the callTrace on calls after a switchover under the following circumstances: When maximum calltrace count is reached before the switchover, and all calls with calltrace enabled are terminated after the switchover. **Root Cause:** The internal calltrace state was not properly synchronized to the standby node that caused no new calls with calltrace ON request can be enabled. **Steps to Replicate:** 1. On a 1+1 (active/standby) SBC set up, set the calltrace count to 10. 2. Create 10 calls with calltrace enabled. 3. Perform a switchover. 4. Terminate the 10 calls after switchover. 5. Perform a switchover. 6. Make new calls with calltrace ON requested in the ADD termination command. These new calls should have calltrace enabled.	The code is modified so that calltrace works after a a switchover. **Workaround:** Reboot both SBC nodes.
24	SBX-109084 | SBX-109214	2	PortFix SBX-109084: The IPv6 SBC traps was not received to the EMS. **Impact:** For trapTargets, certain IPv6 addresses are sent to the incorrect IPv6 address. **Root Cause:** If the IPv6 address, converted to the form of 16 decimal octets separated by periods have a length greater than 47 digits, the address will be truncated. **Steps to Replicate:** Provision an OAM SNMP trapTarget with a customer IP. Observe the tailf snmp.log that the actual address sent to.	The code is modified so the buffer used to store the converted IPv6 string is stored in a buffer of 64 characters, which accommodates any IPV6 address. **Workaround:** None.

25	SBX-109862 | SBX-110925	2	Portfix SBX-109862: The SBC is not rejecting the SRTP call when disallowSrtpStream is enabled. **Impact:** The SBC is not rejecting the SRTP call when disallowSrtpStream is enabled in ingress PSP and Invite is received with only SRTP stream. **Root Cause:** This is specific call flow when disallowSrtpStream is enabled and an INVITE is received with only SRTP stream. This scenario was not handled and the SBC was not rejecting call. **Steps to Replicate:** 1. Feature flag "multipleAudioStreamsSupport" under trunk group media is enabled for both ingress and egress. 2. A disallowSrtpStream flag under trunk group should be enabled on the ingress side. 3. Make a call with two SRTP stream.	The code is modified so that when the disallowSrtpStream is enabled and an INVITE is received with only an SRTP stream, the call is rejected with 488. **Workaround:** None.
26	SBX-109966 | SBX-110950	2	Portfix SBX-109966: The SBC incorrectly accepts an SDP offer in an ACK **Impact:** The SBC is designed to ignore an SDP offer in an ACK, but is not doing so. **Root Cause:** In an early media call, the SIP stack was accepting the SDP in ACK as an offer. This should never happen. **Steps to Replicate:** 1. In an early media call, add SDP in ACK. 2. Send a re-INVITE with SDP from the same side. 3. SIPS stack should ignore the SDP in an ACK and accept the SDP from re-INVITE as an offer.	The code is modified to not forward the SDP to the application. **Workaround:** None.
27	SBX-109298 | SBX-109569	2	PortFix SBX-109298: SBC: The DSP fails to modify ptime. **Impact:** When the SBC receives a re-INVITE with a change in the ptime for EVS, the DSP Modify command fails. **Root Cause:** Handling of DSP Modify Command for ptime change for EVS was not present. **Steps to Replicate:** Run a EVS to G711 call, send a re-invite on the EVS leg with change in ptime. The change in ptime should be put into effect through a DSP Modify.	The code is modified to support for ptime change for EVS is added. Allowable ptime changes include 20, 40, 60, 80 and 100ms. **Workaround:** None.
28	SBX-106127 | SBX-110221	2	Portfix SBX-106127: The SBC product name is incorrect in a 10.0 SBC. **Impact:** The sbcDiagnostic incorrectly prints product name as "ConnexIP5000" instead of "AWS". **Root Cause:** Platform type is determined by querying platform data using dmidecode command, due a bug in the query platform type is returned as unknown. As a result of this bug, the sbcDaignostic shows generic product name ("ConnexIP5000"). **Steps to Replicate:** Run sbcDiagnostic command from the Linux shell of the SBC. It shows the following: **********SBC Information ********* .... SBC Product Name: ConnexIP5000 After a fix, it prints the following: **********SBC Information ********* .... SBC Product Name: AWS	The code is modified to return correct platform type. **Workaround:** No workaround.
29	SBX-109993 | SBX-110007	2	PortFix SBX-109993: The PRS Process is coring with a pkt switchover with a loopback call. **Impact:** The PRS Process core dumped when testing a pkt port switchover. **Root Cause:** The statement to log the debug message was missing a string parameter. **Steps to Replicate:** Force pkt port switchovers. This is intermittent so may be difficult to reproduce.	The code is modified to address the issue. **Workaround:** No workaround.

30	SBX-108956 | SBX-110136	2	Portfix SBX-108956: SBC: Default bitrate for G722 codec should be 64kpbs in SBC but it is 48 kbps. **Impact:** The SBC is using 48kbps bit rate for G722 codec instead of 64kpbs when setting up G722 calls. **Root Cause:** The 48kbps bitrate is incorrectly chosen for G722 codec, resulted in the media packets being generated with 48kbps bitrate. **Steps to Replicate:** Make one g722 to g711 transcode call and observing the RTP stream for g722 codec.	Changed bitrate to 64kpbs when setting up G722 calls to address the issue. **Workaround:** None.
31	SBX-107975 | SBX-110176	2	Portfix SBX-107975: A Serf event processor is unable to restart because restart check marker file is not getting removed. **Impact:** The Serf event processor is unable to restart because the restart check marker file is not getting removed. **Root Cause:** The restart check marker was only being removed if serfeventProcessor starts successfully, so if it fails to start, any attempts to restart it would be prevented because the marker is not removed. **Steps to Replicate:** 1. Make serf event processor fail at some point. 2. It should try to restart up to 5 times if it keeps failing to come up.	The code is modified so that the user can attempt a restart. **Workaround:** None.
32	SBX-105391 | SBX-110222	2	Portfix SBX-105391: SBC: The SM process leaks memory on an OAM active for an SBC switchover. **Impact:** While carrying out operations like a configuration upload to EMS, the memory is leaked. **Root Cause:** The Python/C APIs cause a memory leak while using functions to the upload/download configuration from the EMS. **Steps to Replicate:** Create a direct single instance(ASAN build) registered with EMS, carry out operations saveAndActivate/restoreRevision and change glog /sanitizer_SmProcess* and verify no leaks due to above operation.	Change the implementation from using Python/C APIs to libcurl. **Workaround:** None.
33	SBX-109167 | SBX-110150	2	Portfix SBX-109167: The AddressSanitizer: SEGV on unknown address 0x000000000028. **Impact:** During the pre-parsing the Messagebody, the SEGV on an unknown address is observed in SipsPreParseMsgBody(). This could result in an SCM coredump. **Root Cause:** When the Content-Type is NULL the code was performing string comparisons to see if its an expected Content-Type and the code did not verify that the header pointer was not NULL before accessing it. **Steps to Replicate:** 1. Make an A to B call. 2. Send a re-INVITE with the MessageBody Content-Type as empty.	The code is modified to check the Content-Type string pointer is not NULL before accessing it. **Workaround:** None.
34	SBX-105644 | SBX-110151	2	Portfix SBX-105644: The sonusSbxCertificateExpireSoonWarningNotification trap does not display for all certificates in the current and history alarm lists. **Impact:** The sonusSbxCertificateExpireSoonWarningNotification trap does not display the individual alarms for separate certificates. **Root Cause:** The SBC alarm for sonusSbxCertificateExpireSoonWarningNotification was just using trap ID as key identifier. **Steps to Replicate:** Add multiple certificates to a 1:1 HA system that will expire and configure certificate expiry date. Confirm: • Only one trap is triggered per certificate. • One alarm exists for certificate.	The code is modified to use certificate name as well as trap ID as key identifiers to show the alarm. **Workaround:** None.
35	SBX-109407 | SBX-110061	2	PortFix SBX-109407: MicroFlows are failing in the REGISTER Performance of 2400 RPS (256000 REGISTRATIONS) with an error code 0xf9. **Impact:** Unable to support the 256k concurrent subscriber registrations in Default memory profile for the SBC SWe. **Root Cause:** Existing logic for determination of flow hash causes increased number of hash collisions leading to increased depth of hash buckets, leading buffer starvation. **Steps to Replicate:** 1. Spawn a SBC SWe instance (of default memory config profile). 2. Test the 256K registrations.	The code is modified to minimize hash collisions. **Workaround:** There is no workaround for this.

36	SBX-109424 | SBX-109716	2	Portfix SBX-109424: The SBC sends a 420 Bad Extension response when an INVITE with both supported and require 100rel is sent. **Impact:** The SBC sends 420 Bad extension when Require:100Rel is received in initial Invite and e2e Prack flag is enabled **Root Cause:** Incorrect code was added to reject an INVITE with Require:100Rel when rel100Support flag is disabled and e2e prack flag is enabled. **Steps to Replicate:** 1. The rel100Support must be disabled. 2. The e2e Prack is enabled. 3. An INVITE is received with a Require:100Rel Header.	The code is modified for rejection in the require:100rel scenarios. **Workaround**: Use SMM to remove Require:100Rel Header.
37	SBX-105437 | SBX-109737	2	Portfix SBX-105437: The CDR issues for non-INVITE messages when blacklisting is involved. **Impact:** In case of handling of failure responses for non-INVITE messages, before writing the CDR for a current failure cause code, the SBC was finding out next route and sending a message on network. This worked fine in normal cases as after sending out a request, the response was processed later, after writing a CDR for current failure response. However in a backlisted entry case, no actual message is sent out, so the blacklisted entry CDR was written before the previous CDR response code. **Root Cause:** Whenever a blacklisted entry was involved, the CDR entries were in accurate for this blacklisted entry and the previous entry. **Steps to Replicate:** Configure Routes for non-INVITE as follows: R1 R2 - > Blacklisted R3 R4 -> Blacklisted The CDR's should be printed in order R1, R2, R3, R4 after a fix.	The code is modified to write the CDR for the current failure response code, and later find next route and send a request on the new route. **Workaround:** None.
38	SBX-105175 | SBX-108184	2	PortFix SBX-105175: The SBC sends a re-INVITE while media is played on the ingress side in a GW-GW early media call. **Impact:** In a GW-GW call scenario, while the media is played on the ingress Gateway, the egress SBC is sending a re-INVITE to the UAS. **Root Cause:** Before the ingress GW completes its end to end activation, it received a MODIFY OFFER request from the egress GW due to the change in SDP received in 200 OK for lockdown INVITE. This caused the ingress GW to process modify offer first and then end to end activation later that triggered a re-INVITE towards UAS. **Steps to Replicate:** 1. Send INV from UAC to GW1. 2. GW2 sends INV to UAS. 3. UAS sends 180 SDP. 4. GW1 sends 180 SDP to UAC and starts to play tone. 5. UAS sends 200 OK with out SDP. 6. GW1 sends 200 OK to UAC. 7. GW2 sends ACK and triggers a lock down INVITE. 8. UAS sends 200 OK with change in SDP.	The code is modified so that while modify offer-answer is handled properly during end to end activation. **Workaround:** None.
39	SBX-109418 | SBX-110173	2	Portfix SBX-109418: The LeakSanitizer detected memory leaks Direct leak of 883820 byte(s) in 413 object(s). **Impact:** The SBC was not freeing memory in one of the failure cases. **Root Cause:** The SBC was not freeing memory in few cases where incoming INVITE handling fails. **Steps to Replicate:** 1. Send an INVITE with Replaces having call id, to in the Replaces header that does not match to any existing leg. 2. After the call ends, the ASAN should not show memory leak.	The code is modified to free up memory allocated, in all cases when the INVITE handling fails. **Workaround:** None.

40	SBX-107960 | SBX-109734	2	Portfix SBX-107960: The AWS IPs remain assigned to the standby SBC. Unnecessary dual restarts. **Impact:** If communication between active and standby is broken (over ha0 interface) both assume active roles (split brain). When this happens, the standby node that becomes active calls AWS APIs to move IP address to self. Once ha0 link is restored, the machine that becomes active does not call AWS API to move IP addresses, and this might cause issue when node that has IP does not come up as active. In this case, IPs are assigned on standby and another node becomes active. **Root Cause:** Root cause of this issue is not calling AWS switchover API (move IPs) during split brain recovery. **Steps to Replicate:** Perform a Split brain test and recovery of the SBC HA, and verify that API query is send by an Active SBC after recovery.	The code is modified to call AWS APIs to move IP to current active machine during split brain recovery path. **Workaround:** Manually move all secondary IPs to current active machine to restore calls.
41	SBX-108434 | SBX-109170	2	PortFix SBX-108434: SBC: A Standby OAM fails to come up after the restart of active and standby. **Impact:** After restarting the active and standby or after a fault that causes the SBCs to go down, the standby OAM waits for active to come up first and never recovers if active is down. **Root Cause:** On the Standby OAM startup sequence, there is a makeSureActiveIsUp() loop that exits only after active is up. This results in standby to be in a hung state forever if active is down. **Steps to Replicate:** 1. Start active OAM SBC. 2. Start the standby OAM SBC after 1 minute. 3. Stop the active OAM SBC before it becomes active. 4. The Standby OAM SBC should reboot and recover after 10 minutes.	The code is modified to reboot the instance that is starting as standby, if peer does not become active in 10 minutes. **Workaround:** Reboot the standby OAM SBC to fix the issue.
42	SBX-109017 | SBX-109198	2	PortFix SBX-109017: SBC: Observed MAJOR logs for BRM "BrmAsyncCmdErrHdlr" on T140 load. **Impact:** Occasionally enable-RID errors are seen in NP when the system is subjected to large number of call flows that employ the RTCP termination. **Root Cause:** The message drops in internal queues due to momentary congestion. **Steps to Replicate:** Run an SBC AMRWB<>T140 full load with the RTCP enabled.	The code is modified to ensure the control messages experience a larger queue depth while traversing internal queues. **Workaround:** No workaround.
43	SBX-107646 | SBX-110230	2	Portfix SBX-107646: For a revision not present in the OAM or EMS, upon doing a restore, an error should be thrown. **Impact:** Not showing the proper failed message when failing to download from the EMS. **Root Cause:** The confd was not waiting for the EMS download error as the EMS download was done in a different thread context. **Steps to Replicate:** Case 1: 1. Create 3 revisions on the EMS. 2. Delete the second revision on the OAM and EMS. 3. Request the system admin vsbcSystem restoreRevision revision 2. o/p admin@Rahul-OAM1-192.168.20.13% request system admin vsbcSystem restoreRevision revision 2. This command will restart all nodes unless the target revision is for a previous version of software. Do you want to continue [yes,no] yes result failure reason bundle not found locally or on EMS, unable to view changes for this revision. 4. See the above failure message and no restart of nodes. Case 2: 1. Create 3 revisions on the EMS. 2. Delete the second revision on the OAM. 3. Request the system admin vsbcSystem restoreRevision revision 2. 4. Will observe a restart in all nodes. Case 3: 1. Create 3 revisions on the EMS. 2. Delete the second revision on the EMS. 3. Request the system admin vsbcSystem restoreRevision revision 2. 4. Will observe a restart in all nodes. Any other failure case.	The code is modified to run the restoreRevision procedure on the same thread context. This helps to display proper error in case of failure. **Workaround:** None.

44	SBX-110178 | SBX-110919	2	Portfix SBX-110178: The PRS Process gave heap use after free on address on latest 10.0 build. **Impact:** The PRS Process gave a "heap use after free on address" error while running the HA suite on ASAN build. **Root Cause:** Interface number was being returned after typecasting the main structure to packet LIF structure, and not management LIF structure. **Steps to Replicate:** Run SBX_504_HA suite on ASAN build.	The code is modified to correct the typecasting. **Workaround:** None.
45	SBX-110128 | SBX-110921	2	Portfix SBX-110128: AWS CFN: The SBC auto-registration in the EMS is not working with EMS FQDN. **Impact:** The SBC auto-registration in the EMS is not working when using EMS FQDN. **Root Cause:** A service discovery is unable to resolve the EMS FQDN using a system DNS because there is no ACL rule to allow DNS query to go through. **Steps to Replicate:** 1. Configure the SBC with EMS FQDN. 2. Ensure that it is registering to EMS successfully.	The code is modified to add an ACL rule to allow DNS query to go to the configured nameserver. **Workaround:** None.
46	SBX-104319 | SBX-110138	2	Portfix SBX-104319: There is a conflicted design between two features “sdpRelayAttribute” and “Send RTCP Bandwidth Info”. **Impact:** The SBC sends duplicate b=RR and b=RS attributes when “sdpRelayAttribute” and “Send RTCP Bandwidth Info” are enabled together. **Root Cause:** The SBC skips adding RR/RS to SDP due to "sendRTCPBandwidthInfo" only when “sdpRelayAttribute” is enabled with TFT. Due to this, b=RR and b=RS attributes are added twice in outgoing SDP, when “sdpRelayAttribute” was enabled without TFT. **Steps to Replicate:** Configuration: 1. Enabled sdpAttributesSelectiveRelay flag under TG. set addressContext default zone ZONE_V6 sipTrunkGroup TRUNK_V6 media sdpAttributesSelectiveRelay enabled set addressContext default zone ZONE_V4 sipTrunkGroup TRUNK_V4 media sdpAttributesSelectiveRelay enabled 2. Enabled RTCP with below settings. set profiles media packetServiceProfile DEFAULT rtcpOptions rtcp enable rrBandwidth 500 rsBandwidth 150 Procedure: 1. Make a Basic call such the the bandwidth parameters are received from the endpoint as b=RR:1125, b=RS:775 Expected Result: 1. The SBC should transparently send the b=RR & b=RS parameters in SDP and should not honor the bandwidth configured in the PSP. Also, the SBC should not add duplicate b=RR & b=RS parameters in SDP honoring the configured bandwidth values in PSP.	If “sdpRelayAttribute” is enabled without TFT, and "sendRTCPBandwidthInfo" is also enabled, the SBC does not add the RR/RS due to "sendRTCPBandwidthInfo" since attributes are relayed. **Workaround:** None.

47	SBX-110201 | SBX-110383	2	Portfix SBX-110201: A late offer call resulting in the SBC not sending DTMF for AMR-WB in initial offer towards ingress. **Impact:** The SBC is not sending 16k 2833 Payload type in the initial offer towards ingress during a Late media "convert" call. **Root Cause:** Answer received from egress contained both 8k and 16k 2833 Payload type and that resulted in the SBC incorrectly assigning the 8k PT value to 16k as well while generating offer towards ingress. As a result, the 16k PT get dropped by SIP stack. **Steps to Replicate:** Configuration: Transcode conditional rel100Support enabled honorSdpClockRate enabled DLRBT enabled Configure multiple codecs on both Routes To re-create the issue: 1. The UE initiates Late media convert call. 2. The SBC sends out 180 answer with the below SDP: m=audio 1024 RTP/AVP 96 8 97 0 18 9 101 a=rtpmap:96 AMR-WB/16000 a=fmtp:96 mode-set=0,1,2; mode-change-capability=2; max-red=0 a=rtpmap:8 PCMA/8000 a=rtpmap:97 AMR-WB/16000 a=fmtp:97 mode-change-capability=2; max-red=0 a=rtpmap:0 PCMU/8000 a=rtpmap:18 G729/8000 a=fmtp:18 annexb=no a=rtpmap:9 G722/8000 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 Test Result without a fix: The SBC drops the telephone-event/16000 payload type when generating offer towards ingress in 180.	The code is modified to prevent the same PT value getting assigned to both 8k and 16k DTMF in this call flow. **Workaround:** None.
48	SBX-106693 | SBX-110228	2	Portfix SBX-106693: SBC: There was a wrong warning message on the Direct-SBC while doing restore. **Impact:** The wrong warning message was displayed during a restoreRevision. **Root Cause:** Rewording of the text message required for when restorerevision was invoked. **Steps to Replicate:** 1. A new image was created after changes. 2. The new csar file was loaded to VNF Manager. 3. Created revision 2 on the EMS. 4. Run the command "request system admin vsbcSystem restoreRevision revision 1". test output admin@Rah-OAM1-192.168.20.3% request system admin vsbcSystem restoreRevision revision 1 This command will restart all nodes unless the target revision is for a previous version of software. Do you want to continue [yes,no]	The code is modified by rewording the warning text message. **Workaround:** None.
49	SBX-110362 | SBX-110363	2	PortFix SBX-110362: The SBC generates RTP inactivity alarms when the policer mode is set to bypass. **Impact:** The SBC generates false RTP inactivity alarms when the policer mode is set to bypass. **Root Cause:** A bug in the media policing logic of SWe_NP code skips updating the timestamp of last RTP packet of a media flow, resulting in raising RTP inactivity notifications for every 10 seconds. **Steps to Replicate:** 1. Configure a ISBC instance. 2. Set the policer mode to bypass (Unit tested by hacking the code). 3. Configure RTP inactivity. 4. Run the call for more than the rtp inactivity duration. 5. Observe that RTP inactivity alarms being raised, even if traffic flow is happening.	The code is modified to update the timestamp after every arrival of RTP packet for the media flow. **Workaround:** Ensure the policer mode is set values to other than 'bypass".

50	SBX-110054 | SBX-110432	2	Portfix SBX-110054: The encrypted packets not being sent towards racoon in case of IPsec tunnel mode. **Impact:** The lawful Interception fails when IPsec is enabled for LI media over UDP. **Root Cause:** An earlier fix assumed the LIG information to be stored in the selector structure to send notification to XRM, indicating if a IPsec tunnel is for LI media. The field was LIG was present in the selector but was never updated. This resulted in failure to send notification to XRM to indicate IPsec tunnel for LI media, for it always failed the match with the LIG configured under the CDC and as a result, the LI failed. **Steps to Replicate:** 1. Generate Local and remote Certificates which has FQDN as a SAN value and signed by an Intermediate CA. 2. Copy Intermediate CA's and Racoon's .crt files to /opt/sonus/external on SBC. 3. Covert Remote Files to .der and local files to .p12. 4. Configure IPSEC related configuration on SBC. 5. Execute a basic call over IPSEC interface. Expected Results: 1. CA, Local(SBC) and Remote(Racoon) certificate generated successfully. 2. Copy of certificate files to SBC is successful. 3. Conversion of remote and local certificate is successful. 4. All configuration issuccessful. 5. IMS LI is configured successfully. 6. Basic call must run successfully over ipsec enabled interface. Signaling and media are captured on IMS LI	The LIG check is removed to ensure that the notification is sent to XRM to indicate the IPSEC Tunnel is for LI media. **Workaround:** No workaround.
51	SBX-102618 | SBX-109302	2	PortFix SBX-102618: The SBC needs to handle the scenario where member-join event handling is missed at the serf level. **Impact:** A race condition in RGM event handling can show sync to be inProgress in N:1. **Root Cause:** A race condition in handling member-join event causes some member-join events to get discarded at serf level. **Steps to Replicate:** Perform multiple sbxrestarts but it is not readily reproducible.	The code is modified to ensure the Redundancy Group is up-to-date. **Workaround:** None.
52	SBX-106589 | SBX-110493	2	Portfix SBX-106589: The SBC SWe does not forward the SIP Info and drops the call. **Impact:** After receiving 32763 SIP indialog INFO messages, the SBC sends a 500 error for further INFO messages instead of forwarding the message. **Root Cause:** The SBC maintains the callHandle structure with refcount, which will be incremented for every reference and decremented once reference is released. But in this case, the refcount is not decremented properly, for every indialog msg (INFO) request received, the count kept increased. **Steps to Replicate:** 1. Establish a call. 2. Send indialog INFO messages more than 32763.	The code is modified to address the issue. **Workaround:** No workaround.
53	SBX-106897 | SBX-110224	2	Portfix SBX-106897: The SBC does not send notify for successful trace activation. **Impact:** The SBC does not send a calltrace notify to C3 in a call setup with calltrace ON request for ADD commands of both first termination and second termination of the call, but the ADD command failed for the second termination. **Root Cause**: The SBC code logic was to send a calltrace NOTIFY after the ADD commands of both termination have been processed, but this result in calltrace NOTIFY not sent for the first termination in failure of ADD in the second termination. **Steps to Replicate:** 1. Enable calltrace in the SBC. 2. Send ADD request with CALLTRACE/TRACEACTIVITYREQUEST=ON on both the terminations. The codec should be PCMU on the first termination and G726 on the second termination, such that ADD of second termination will fail (not supported codec). Expect Result: 1. The call fails. 2. The SBC sends calltrace NOTIFY with RES=success for the first termination.	The code is modified to send calltrace NOTIFY for successfully ADDed termination. **Workaround:** None.

54	SBX-109439 | SBX-110914	2	Portfix SBX-109439: SBC: An activeRevision failure when state for even type audit is set to on/off. **Impact:** The configuration Playback on managed VMs fails on command. set oam eventLog filterAdmin vsbc1 audit audit level major state off **Root Cause:** The playback engine does not use user context. **Steps to Replicate:** Run the command on the OAM. set oam eventLog filterAdmin vsbc1 audit audit level major state off commit Perform a saveAndActivate.	The code is modified to address the issue. **Workaround:** Reboot on managed VMs to get the configuration at startup.
55	SBX-109412 | SBX-110910	2	Portfix SBX-109412: The destination buffer was too small during the snprintf function. **Impact:** During the snprintf function call, the destination buffer was not big enough to copy the source string. **Root Cause:** The size of the destination buffer was smaller than the source buffer because the destination buffer length check was not present. The buffer file size should be 256 bytes. File: call/sonus/p4/ws/jenkinsbuild /sbxAsan100/marlin/SIPS/sipsParse.c **Steps to Replicate:** 1. When the callId length was more then the defined max callId length this error was seen. 2. Run a call with callId length greater than 256 bytes. This error should not come.	The code is modified to address the issue. **Workaround:** None.
56	SBX-109453 | SBX-110622	2	Portfix SBX-109453: The SBC is closing the socket for DNS query over TCP frequently. **Impact:** The SBC is closing the socket for DNS query over TCP frequently. **Root Cause:** Whenever the TCP connection is closed, the FIN packet is sent towards the SBC from DNS server. But the application was not closing the connection by sending the FIN and Even after a connection is closed by DNS server, the application is still holding socket information. This details were used in future queries has cause TCP connection to reset. **Steps to Replicate:** 1. Have a v6 Cloud SBC with the below build SBC: V10.00.00-A006. 2. Configure the DNS server to send queries using TCP connection. 3. Make a call. 4. Wait for some time and run one more call here. Actual behavior: In step 3, the SBC will query DNS server to resolve NAPTR records over TCP connection. In step 4, the SBC will try to send a NAPTR query and then immediately close TCP connection. Expected result: The NAPTR query should be successful in step.	The code is modified to close TCP connection (Sending FIN to close connection). Also, the connection information in application is freed. **Workaround:** No workaround.
57	SBX-106520 | SBX-106881	2	PortFix SBX-106520: Among the exported setting values, there were setting values that were not set in other environments. **Impact:** The "comment" parameter is missing from some configuration related to AAA rules/cmdRules. **Root Cause:** The "comment" parameter is not being restored during a LSWU. **Steps to Replicate:** 1. Spawned a SBC, exported the configuration and observed comment parameters are present. 2. Upgraded the SBC software. exported the configuration and observed comment parameters are not present. Revised the steps above with fix, and the issue was not observed.	The code is modified to restore "comment" parameter during a LSWU. **Workaround:** None. The "comment" parameter is used only for description. It doesn't have functional impact.

58	SBX-106869 | SBX-110296	2	Portfix SBX-106869: The SBC Node branch information is inconsistent after a Cleanstart/Restore Revision is performed in OAM's. **Impact:** The SBC Node branch information is inconsistent after the Cleanstart /Restore revision is performed for OAMs. **Root Cause:** Managed VMs registration failed with active and standby OAMs as OAMs were not up. VMs did not retry to register again. **Steps to Replicate:** After the issue is fixed, create a setup OAM and S/M/T SBC. 1. Log in to the CLI as admin and execute the following: show configuration node o/p: All nodes should be listed. 2. Configure the SBC (create AddressContext, zone, TG) saveAndActivate Revision o/p: new configRevision should be propagated to all managed VMs.	The code is modified to keep retrying to register with active and standby OAMs. **Workaround:** None.
59	SBX-108112 | SBX-109576	2	PortFix SBX-108112: MS TEAMS - The Media Stats are not correct when the DLRBT profile is removed from TGs and ICE is enabled. **Impact:** On an SBC was configured for MS Teams LMO centralized mode with ICE, if DLRBT is not correctly configured, this can lead to media not flowing correctly for a call even after ice learning gets completed. **Root Cause:** The early ICE learning logic for non DLRBT mode in the SBC was not fully deactivating ICE media resources on receipt of 200 OK . As a result, the resources were unable to be re-activated for end to end media flow. **Steps to Replicate:** On an SBC configured as MS Teams LMO centralized mode with ICE on MS Teams TG: 1. Disable DLRBT on PSTN and MS Teams TG's. 2. Establish a PSTN endpoint to MS Teams call that uses primary (Internal) LIF address towards Teams. 3. Once call has established and ice learning has completed, send media (voice) in both directions between PSTN and Teams endpoints. 4. Media should flow as expected in both directions and call Media status should correctly show the number of media packets sent and received for ingress and egress.	The code is modified to correctly deactivate early ice learning media resources on receiving an SDP from MS Teams. **Workaround:** The DLRBT should be enabled.
60	SBX-109220 | SBX-110005	2	PortFix SBX-109220: The monitor.c "runtime error: signed integer overflow: 0 - -9223372036854775808 cannot be represented in type 'long int'" error in the np. log. **Impact:** Internal ASAN builds report runtime signed integer overflow error in SWe for standard deviation metric for jitter meant for consumption by Ribbon Protect. **Root Cause:** Existing algorithm of standard deviation metric did not handle integer overflow issues. **Steps to Replicate:** Stream the custom RTP packet where expected standard deviation and verify via Ribbon Protect metric that computed standard deviation values are in range.	The code is modified to handle the overflow. **Workaround:** No workaround. This metric is only exposed to Ribbon Protect. This is not exposed as a metric in any SBC display or CDR.
61	SBX-70800 | SBX-109606	2	PortFix SBX-70800: AWS:Observing that metaVariable table is getting modified on the loading the backup configuration file of one instance in other instance. **Impact:** When loading the backup configuration from one SBC instance to another, the metavar table is getting populated with the list of metavars from both instances. This by itself does not cause any issues so long as the metavars are unique, it is incorrect to see the metavars for another instance in the table. **Root Cause:** The code was not removing the existing metavars prior to loading the configuration of another instance. This meant the metavar table had both sets of information. **Steps to Replicate:** 1. Create a backup configuration of one cloud instance (instance1). 2. Loaded the backup configuration file into a new cloud instance (instance2). 3. Check the metaVariables table and see if it contains the metavars from both instances.	The code is modified to flush the metavars for the existing instance prior to loading the configuration from another instance. **Workaround:** None.
62	SBX-108577 | SBX-109166	2	PortFix SBX-108577: The CE_2N_Comp_SmProcess==11649==ERROR: AddressSanitizer: SEGV on an unknown address 0x000000000000. **Impact:** The SBC was performing a write operation on one of the un-allocated memory space while restoring NTP server configuration. As a result, SEGV on unknown address was reported. **Root Cause:** This issue was caused because a flag variable was not initialized. As a result, if condition was evaluated true instead of false, a write operation would be performed. **Steps to Replicate:** Configuring the NTP server and restoring the configuration by switchover or restart this error should not come up.	The code is modified to address the issue. **Workaround:** None.

63	SBX-106759 | SBX-110175	2	Portfix SBX-106759: In a N:1 mode, the SBC performs a switchover for a different node than the switchover request is honored for. **Impact:** In N:1 during few scenarios, SBC switchovers to node that was not request honored. When the issue occurred, a switchover will be processed to other node instead of processing to request honored node. **Root Cause:** During switchover process SBC was not checking the node which was requested honored. It was switching over to a node that comes first/is available while processing in the SBC. **Steps to Replicate:** 1. Bring up a 2:1 SBC. 2. Try to reboot the both active server. 3. While switchover process delay the up of request honored node and allow the another node to come up first.	The code is modified to check the service id of the request honored node before a switchover. **Workaround:** None.
64	SBX-106613 | SBX-110297	2	PortFix SBX-106613: The SBC adds duplicate header on new INVITE upon 422 response, when a transparency profile is attached to egress TG. **Impact:** The SBC adds a Duplicate Header on a new INVITE after the 422 Response is received. **Root Cause:** The SIP Stack adds a semi-known twice (Header is unknown to SIP Parser but configured in transparency Profile) in this 422 scenario. **Steps to Replicate:** 1. Header has to be unknown to the parser. 2. The same header name needs to configured in the Transparency profile.	The code is modified to Skip formatting the second instance of same header based on header type. **Workaround:** SMM can be added to remove the duplicate header.
65	SBX-110246 | SBX-111002	2	PortFix SBX-110246: The OAM and SBC nodes would not start after revert to 9.1 from 10.0. **Impact:** The SBC node fails to start after reverting from 10.0 to 9.1. **Root Cause:** The start-up failure after the SBC node revert from 10.0.0 to 9.1 is due to incorrect permissions of logs in /var/log/postgresql/ directory. **Steps to Replicate:** Perform revert from 10.0.0 to 9.1 on the SBC node and verify the SBC comes up fine post revert.	The code is modified to update the right permissions on files in /var/log/postgresql/ directory after revert. **Workaround:**
66	SBX-107973 | SBX-110017	2	Portfix SBX-107973: The SBC adding RR and RS attributes twice in the egress INVITE when multiple m lines present in SDP. **Impact:** The SBC was adding RR and RS attributes twice in the egress INVITE when multiple m lines present in a SDP. **Root Cause:** The SBC is not setting the default value of M lines present in SDP when number of lines is greater than 1 and as a result, the SIPS value is getting added. **Steps to Replicate:** Configure these: set profiles media packetServiceProfile DEFAULT rtcpOptions rtcp enable set profiles signaling ipSignalingProfile DEFAULT_SIP commonIpAttributes flags sendRTCPBandwidthInfo enable set profiles signaling ipSignalingProfile DEFAULT_SIP commonIpAttributes flags sendRtcpPortInSdp enable comm set addressContext default zone ZONE_EGRESS sipTrunkGroup TG__EGRESS media multipleAudioStreamsSupport enabled set addressContext default zone ZONE_INGRESS sipTrunkGroup TG_INGRESS media multipleAudioStreamsSupport enabled comm An incoming INVITE has multiple Audio line with: b=RS:250 b=RR:250	The code is modified so that if value is set to default and it is not getting modified, the SIP does not send the RR and RS value twice. **Workaround:** When the sdpAttributesSelectiveRelay is enabled, the SBC does not send RR and Rs twice.
67	SBX-108008 | SBX-110137	2	Portfix SBX-108008: SBC: Observed MAJOR logs with MegacoSendAmmsResp failure after a switchover during an EVS and T140 -> Mulaw Load. **Impact:** There was a MegacoSendAmmsResp: MegacoSendAmmsResp: Failure while encoding the response, and Error code = 197 Major logs observed after a switchover of the SBC during a load run of call setup with audio and text stream. **Root Cause:** The text stream is not properly synchronized to the standby node and triggers the h248 message encoding error in reply to a H248 MODIFY command. **Steps to Replicate:** Perform failover during call load run with EVS and ToIP on ingress side and the G711U+Baudot on egress side.	The code is modified to address the issue. **Workaround:** None.

68	SBX-107142 | SBX-108456	2	PortFix SBX-107142: The SBC VM was unable to power on a post power off procedure. **Impact:** The VMware GPU SWe instance does not come up post reboot or GPU is not visible in the instance. **Root Cause:** When the SWe instance runs in GPU mode, the persistence mode of the NVIDIA driver is enabled using the nvidia-smi to prevent the GPU state from being unloaded. This is a kernel-level solution and creating problem when the hypervisor is VMware. **Steps to Replicate:** 1. Set sweActiveProfile to use GPU. 2. Reboot the instance after the SBC application is up. RESULT: Instance should come up and GPU should be visible in the instance.	The code is modified to address the issue **Workaround:** No workaround.
69	SBX-105457 | SBX-110171	2	Portfix SBX-105457: An error is thrown on the EMA while configuring the SMM Profile having messageBody criteria with regex. **Impact:** An error is thrown on the EMA while configuring the SMM Profile having messageBody criteria with a regex. **Root Cause:** The EMA assumes that the Num Match was a mandatory field but it is an optional field (user may enter that value or he may not). **Steps to Replicate:** 1. Log into the EMA. 2. Navigate **profile** -> **signaling** -> **sip adaptor profile** 3. Create the profile that should have a Num match value and after that delete the Num Match value from the CLI. 4. As a result, you cannot see the issue.	The code is modified to make the Num Match field optional. **Workaround:** None.
70	SBX-107639 | SBX-110135	2	Portfix SBX-107639: The CA CMR with offset 2 and priority LOW is not being processed or rejected. **Impact:** When a Channel Aware (CA) Mode CMR for priority LOW and offset 2 was the first CA CMR received in a call, the CMR was not processed. **Root Cause:** The present default value of curFecIndOffset in the code was set to 0 that corresponds to offset 2 and priority LOW. Due to this default value when a CMR for offset 2 and priority low is received as the first CA CMR, it is not getting processed. **Steps to Replicate:** Test 1: 1. Enable IR9.2cmr in the SBC. 2. Send ADD request with A1 profile having ch-aw-recv=-1 parameter in T1 termination. 3. Pump pcap with 13.2br with cmr byte of CA-L-O2 followed by CA-H-07 Expected Result: 1. The SBC should accept the ADD request. 2. The SBC should not accept the cmr request. InvalidCMRCount should be incremented Actual Result: 1. The call is successful. 2. invalidCMRCount gets incremented as per the number of invalid CMRs received Test 2: 1. Enable IR9.2cmr in the SBC. 2. Send ADD request with A1 profile having ch-aw-recv=0 parameter in T1 termination. 3. Pump pcap with 13.2br with cmr byte of CA-L-O2 followed by CA-L-03 Expected Result: 1. The SBC should accept the ADD request. 2. The SBC should accept the cmr requests. codecModeChangeRxCnt should be incremented to 2.	The code is modified so that the default value does not match any of the valid curFecIndOffset that is 0-7. **Workaround:** None

71	SBX-108232 | SBX-110929	2	Portfix SBX-108232: SBC: The AddressSanitizer: detected a heap-use-after-free on address 0x61800000a5a8 at pc 0x559e8989c4ac bp 0x7f4411fde290 sp 0x7f4411fde288 READ of size 8 at 0x61800000a5a8 thread T9. **Impact:** While the SBC node is shutting down it can access memory after its been freed, this could result in unexpected behaviour and in the worst case a coredump. But would have limited impact as it only happens when shutting down. **Root Cause:** During a sbxstop/sbxrestart or switchover because of race-condition, when the SBC is in deactivation the oamNodeRegisterRetry can access already deallocated resource leading to a core dump. **Steps to Replicate:** 1. Setup build with HA SBC using OAM. 2. Perform a sbxrestart/switchover of active instance.	The code is modified to handle this race condition. **Workaround:** None.
72	SBX-109443 | SBX-109675	2	PortFix SBX-109443: ERROR: The AddressSanitizer: detected heap-use-after-free on address 0x61900412bbce at pc 0x55d0b8c48037 bp 0x7fb50a457b00 sp 0x7fb50a4572b0 READ of size 2 at 0x61900412bbce thread T11. **Impact:** The ASAN reported "AddressSanitizer: heap-use-after-free" error for subscribe message received with Proxy-Authorization header having auts parameter. Ex: Proxy-Authorization: Digest auts*="0x01P+20" **Root Cause:** An invalid access of the freed memory occurred in this case. Accessing memory after it is freed can cause unexpected behavior that may result in coredumps. **Steps to Replicate:** Send a SUBSCRIBE message received with Proxy-Authorization header having auts parameter.	The code is modified to address the issue. **Workaround:** None.
73	SBX-109186 | SBX-110422	2	Portfix SBX-109186: [ASAN]: sanitizer.CE_2N_Comp_SamProcess.32180: /localstore/ws/jenkinsbuild/sbxmainasan/marlin/TRM/trmTgPsStat.c:1427:74: runtime error: signed integer overflow: -2147061904 - 552880 cannot be represented in type 'int' **Impact:** There was a runtime error: signed integer overflow. **Root Cause:** A runtime error occurred due to wrong type casting from ULONG to LONG. **Steps to Replicate:** Run the codenomicon INVITE response with outgoing bye codenomicon UAC suite.	The code is modified to address the issue. **Workaround:** None.
74	SBX-104817 | SBX-109818	2	Portfix SBX-104817: The SBC does not answer the SDP correctly when the remote SDP contains both session and media port state attributes. **Impact:** The SBC sets incorrect media port state in the SDP in reply of a MODIFY command when media port state is present in both session level and media level. **Root Cause:** The SBC parsed the media port state incorrectly when it is present in both session level and media level, and put them both at media level in the reply SDP. **Steps to Replicate:** Create a 3pcc call, then send a re-invite that triggers C3 sending a MODIFY with media port state present in both session level and media level. The SBC should keep them the same session level and media level in the SDP in the reply.	The code is modified when parsing media port state attribute when it is in both session level and media level. **Workaround:** None.
75	SBX-109209 | SBX-110139	2	Portfix SBX-109209: SBC: Observed MAJOR logs for SIPFE "/localstore/ws /jenkinsbuild/sbxMain/marlin/SIPFE/sipFeSigPortCsv.c, SipFeGetSipSigPortStatisticsGetNextReqMsg, 1111] Another Query in process" on T140 load. **Impact:** Observed MAJOR logs for SIPFE "/localstore/ws/jenkinsbuild/sbxMain /marlin/SIPFE/sipFeSigPortCsv.c, SipFeGetSipSigPortStatisticsGetNextReqMsg, 1111] Another Query in process" on T140 load. **Root Cause:** The addressContext zone sipSigPortStatistics table is not supported on the SBC, so the code used to return the information was sometimes not returning, causing the error messages above. **Steps to Replicate:** 1. Run the following command: snmpwalk -c admin -v2c <mgmt address of sbx> 1.3.6.1.4.1.2879.2.10.2.121 Repeat this command 4 times. 2. Verify the following error: "/localstore/ws/jenkinsbuild/sbxMain/marlin/SIPFE/sipFeSigPortCsv.c, SipFeGetSipSigPortStatisticsGetNextReqMsg, 1111] Another Query in process" on T140 load Does not occur in the DBG log.	The code is modified so SipFeGetSipSigPortStatistics routines return immediately. **Workaround:** Do not query that table.

76	SBX-109187 | SBX-109266	2	PortFix SBX-109187: [ASAN]: sanitizer.CE_2N_Comp_ScmProcess_0.32472: /localstore/ws/jenkinsbuild/sbxmainasan/marlin/SIPS/sipsParseActions.c:16242: 70: runtime error: null pointer passed as argument 2, which is declared to never be NULL. **Impact:** The NULL pointer was accessed during the codenomicon test with an ASAN SBC build. **Root Cause:** The Codec Attribute has been accessed in the SDP without a proper NULL check. **Steps to Replicate:** 1. Install the ASAN build on the SBC. 2. Run Codenomicon INVITE response with the outgoing Bye suite.	The code is modified to add the defensive NULL check. **Workaround:** Not applicable.
77	SBX-108619 | SBX-110145	2	Portfix SBX-108619: [ASAN]: /localstore/ws/jenkinsbuild/sbxmainasan/marlin/SIPS /sipsPreParse.c:1742:46: runtime error: signed integer overflow: 2002002002 * 10 cannot be represented in type 'int'. **Impact:** A runtime error is seen in the SAM process. When an INVITE is sent out and response code received is very large, we will see the following issue: Runtime error: signed integer overflow: cannot be represented in type 'int' **Root Cause:** When the SIP Response code is very large, there is a signed integer overflow during the processing of the SIP PDU. **Steps to Replicate:** An INVITE is sent out to the egress. If the response code received is very large, the issue is seen.	The code is modified so if the SIP response is greater than or equal to max response code, the SBC throws an error. **Workaround:** None.
78	SBX-108572 | SBX-110148	2	Portfix SBX-108572: [ASAN]: /localstore/ws/jenkinsbuild/sbxmainasan/marlin/SIPS /sipsParseActions.c:12698:76: runtime error: index 20 out of bounds for type 'sip_nameval_str [20]' **Impact:** When the PUBLISH message is received with 20 params in the Contact Header, the SBC throws a runtime error: index 20 out of bounds for type 'sip_nameval_str. **Root Cause:** The param check for boundary condition was missing while parsing the contact header. While it was checking the params, the number of params should be less than 20, but the condition to handle number of params is not specified. **Steps to Replicate:** Send a PUBLISH message with 20 or more params in the Contact header.	The code is modified so if the number of params is 20, the SBC should throw a parse error. **Workaround:** None.
79	SBX-108411 | SBX-110024	2	PortFix SBX-108411 : [ASAN]: sanitizer.CE_2N_Comp_ScmProcess_2.30828: ==CE_2N_Comp_ScmProcess_2==30828==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61b00008dc88 at pc 0x5621c53c6946 bp 0x7f9854100bc0 sp 0x7f9854100bb8. **Impact:** While running a INVITE CANCEL Proxy Call, the UAS observed a Address Sanitizer leak in SCM process and the SBC services stopped. **Root Cause:** Issue in parsing string when string is blank and very large that lead to a heap buffer overflow. Example: SIP/2.0/UDP 10.xx.xx.xx:7009;sigcomp-id=" LWS " When the token length becomes large 100 say (which is the LWS length) and this token length point outside the PDU, we will see this issue. **Steps to Replicate:** Send an INVITE with a VIA header as the last header.	The code is modified to use temptokLen instead of the tokLen. As a result, the tokLen does not reach outside the PDU. **Workaround:** The VIA header should not be last header, and the empty token string should be small.
80	SBX-109873 | SBX-110385	2	Portfix SBX-109873: The SBC includes the "text port = 0" in its response for the re-INVITE to insert the text at the mid call. **Impact:** The SBC rejects the t140 stream in handling a MODIFY command that changes the audio codec from PCMU to AMR-WB and a t140 stream, with "adaptive codec" enabled. **Root Cause:** The SBC delays the process of MODIFY command when "adaptive codec change" is enabled, and as a result the MODIFY reply is sent back to C3 without t140 stream media resource allocation (IP and RTP port, etc). **Steps to Replicate:** With an adaptive codec change enabled on a VMG, create a 3pcc call from EVS + t140 — PCMU + t140. Then MODIFY T2 side to AMR-WB + t140 and the SBC should reply with a valid port number for t140 stream.	The code is modified to address the issue. **Workaround:** None.
81	SBX-108410 | SBX-109379 | SBX-110155	2	PortFix SBX-108410: [ASAN]: sanitizer.CE_2N_Comp_ScmProcess_3.8866: ==CE_2N_Comp_ScmProcess_3==8866==ERROR: AddressSanitizer: heap-use-after-free on address 0x6190001c77dd at pc 0x558bcc9ff877 bp 0x7fea305f4e00 sp 0x7fea305f45b0. **Impact:** The ASAN reported a "AddressSanitizer: heap-use-after-free" error when Subscribe request having a NULL character in quoted string. **Root Cause:** Invalid access of the freed memory occurred. Accessing memory after it is freed can cause unexpected behavior that may result in coredumps. **Steps to Replicate:** The codenomicon subscribe-notify suite.	The code is modified to now log a parser error. **Workaround:** None.

82	SBX-108574 | SBX-110908	2	Portfix SBX-108574: [ASAN]: CE_Node2.log:snprintf buffer too small. Need 327 Have 128 File: /localstore/ws/jenkinsbuild/sbxmainasan/marlin/SIPSG /sipsgLibUtils.c Line: 2524. **Impact:** The length of the destination buffer was smaller than the source buffer while calling the snprintf function that why buffer too small error was seen. **Root Cause:** The destination buffer size was smaller than the source buffer while calling snprintf. **Steps to Replicate:** Run publish requisition codenomicon test suite. This error should not come.	The code is modified to upper limit of source buffer size. **Workaround:** None.
83	CHOR-7443 | SBX-107356	2	PortFix CHOR-7443: Call failures are observed with a 503 error response due to UXPAD process utilization spiked to 20% more that causes overall CPU usage of media container reaches above 90% utilization. **Impact:** CPU congestion was observed for media core in 2 VCPU scenarios, leading to call failures. **Root Cause:** There was a scheduling issue between NP and UXPAD running on the same core that was causing random spikes of processes causing media congestion. **Steps to Replicate:** 1. Create a 2 VCPU scenario in public cloud and run transcode heavy load. (This issue was seen specifically in container environment where we do not have much control on performance tuning parameters). 2. Run the load for 2-3 days. 3. Check if there are any call failures due to media core CPU congestion during the execution.	The code is modified to adjust the process priority of NP and UXPAD to have better scheduling and avoid spikes of processing. **Workaround:** None.
84	SBX-105073	2	The *XrmAsyncCmdErrHdlr: ERROR NpMediaIntf cmd 2c gcid. **Impact:** The set grace command returned an error code 0xF0 from the NP, which triggered unsolicited call cleanups. **Root Cause:** The set grace command can only be performed on a disabled media flow in the NP. But, thet NP had received some set grace commands issued on an already enabled media flow. Unfortunately, we are unable to determine from just the core WHY XRM and NP became out of sync. **Steps to Replicate:** The issue is not reproducible. Perform regular regression tests.	The code is modified to set after XRM has sent media flow enable command to NP and is cleared on media flow disable. The XRM checks this flag and only send set grace commands to NP when this flag is clear. If the flag is set, the XRM reads the media control block in NP and log a MAJOR level debug message to help future debugging efforts. Similarly introduced a set of new flags in the BRES structure for RTCP Gen enable/disable commands sent to NP. The BRM checks the new flags and only enables RTCP Gen in NP when the flag is clear. If the flag is set, BRM reads the rtcpGen control block in NP and log a MAJOR level debug message to help future debugging efforts. **Workaround:** No workaround.
85	SBX-108369	2	The FIPS mode was broken on the AWS SBC. **Impact:** After enabling the FIPS mode on the AWS SBC or OpenStack, the SBC functions such as 'certificate import' do not work. **Root Cause:** While enabling FIPS mode, the FIPS flag is set in sbx.conf. But on Openstack/AWS deployments, the sbx.conf gets reset on the reboot causing a reset of the FIPS flag. **Steps to Verify Fix:** 1. Enable fipsMode from CLI. 2. After a reboot, check /opt/sonus/conf/sbx.conf or try a certificate import from the CLI. The fipsMode in sbx.conf is set to 'enabled'.	The code is modified to retain FIPS flag in sbx.conf on reboot. **Workaround:** After enabling the FIPS mode, set fipsMode=enabled in /opt/sonus/conf/sbx.conf.reconfigHa.orig and reboot the SBC. After a reboot check, /opt/sonus/conf/sbx.conf
86	SBX-109105	2	OOD PUBLISH vs. OOD INFO: There are different NRM triggers/congestion profiling. **Impact:** OOD PUBLISH vs. OOD INFO: There are different NRM triggers used for congestion profiling. **Root Cause:** Some of the OOD message types were not being included for triggering NRM congestion. **Steps to Replicate:** Run with carious OOD PUBLISH and INFO messages that should trigger NRM congestion and calculate CPS resource appropriately.	The code is modified to trigger the NRM congestion by including all OOD message types. **Workaround:** There is no workaround.

87	SBX-109493	2	Forwarding info was redirecting info for a customer. **Impact:** When testing with JJ90.30 call flows and sending in the following parameters, the RDI (redirection information) parameter created from the history header information had the redirecting indicator field set to “call diverted, all redirection information presentation restricted” even though there was no privacy parameter information in the history header. **Root Cause:** The SBC interworking code was following the 3GPP 29.163 specification table 7.4.6.3.2.3 that allows the standard SIP privacy header information to be used when setting the RDI parameter information. Due to the setting RDI parameter information "id", it resulted in the redirecting indicator parameter value of “call diverted. All redirection information presentation restricted” instead of it being set to "call diverted". **Steps to Replicate:** Send an INVITE to the SBC, with parameters similar to those in the impact statement and check in the policy request that the RDI redirecting indicator field is set to "call diverted". The SIP trunk group variant needs to be set to TTC and the signaling acceptHistoryInfo control needs to be set to enabled.	The code is modified to not consider the SIP Privacy header value when determining the RDI parameter redirecting indicator field value if the SIP trunk group variant is set to TTC. **Workaround:** None.
88	SBX-109013	2	Increased the healthcheck interval. **Impact:** Core dumps are occasionally seen in the field due to the health check timer expiring when the process gets stuck. **Root Cause:** In SWe environments, disk/CPU timing issues can lead to the process slowing down and hitting these health checks. **Steps to Replicate:** This issue was only reproduced using debug code.	The code is modified to be more forgiving to cope with short spikes. The health check ping interval is now 2 seconds and needs to have 15 consecutive non responses in order for the process to be declared deadlocked and a coredump initiated to recover. **Workaround:** None.
89	SBX-106788	2	TOD Routing broken for non-ALL timeRangeProfiles **Impact:** Time of Day Routing is broken for any configured time range profile other than the default ALL profile **Root Cause:** The time of the day values are stored in the DB as hexadecimal octets and A to F digits are stored as lower case. While matching the configured data, the stored values are compared against upper case A to F digits, thus the result of this match always failed. **Steps to Replicate:** Set timeRangeProfile other than ALL to test. set global callRouting route trunkGroup INTERNAL_IPTG99 VSBCSYSTEM standard Sonus_NULL 1 all all TEST0001 none Sonus_NULL routingLabel TO_EXTERNAL_TG99 Note, the TRP TEST0001 is defined as below, and is set to match all days and all times: set profiles callRouting timeRangeProfile TEST0001 entry 7 timeZone psxLocal set profiles callRouting timeRangeProfile TEST0001 entry 7 dayMatching dayOfWeek monday,tuesday,wednesday,thursday,friday,saturday,sunday set profiles callRouting timeRangeProfile TEST0001 entry 7 dayMatching holidays disable set profiles callRouting timeRangeProfile TEST0001 entry 7 dayMatching specialDays range none set profiles callRouting timeRangeProfile TEST0001 entry 7 timeMatching range all	Code is updated in the matching function to check for both lower case and upper case hexadecimal digits. **Workaround:** No workaround
90	SBX-110719	2	HA setup on ASAN is not coming up after call config - pathcheck & SMM **Impact:** While testing with the following configuration the code could potentially read of the end of an internal memory block while printing a debug log. In the worst case scenario this could result in an SCM coredump. set addressContext default zone <zonename> sipTrunkGroup <trunk group> signaling messageManipulation smmProfileExecution fixedOrder **Root Cause:** The internal structure was not always getting initialized correctly prior to trying to print the contents and this led to the code reading pass the end of the memory block. **Steps to Replicate:** Configure SMM with the fixedOrder configuration and make some calls. This issue was highlighted while running with ASAN images in the engineering lab.	The code has been updated to correctly initialise the internal structure and avoid reading past the end of a memory block. **Workaround:** Avoid using the "signaling messageManipulation smmProfileExecution fixedOrder" configuration if possible.
91	SBX-111059	2	Memory leaks are observing on ASAN build when SMM is configured **Impact:** While assigning SMM or flexible policy profiles to the zone configuration small amounts of memory leaked. **Root Cause:** The code was allocating memory in order to read information from CDB as part of processing the assignment and the memory did not get freed up at the end of processing. **Steps to Replicate:** Make SMM configuration changes at the zone level.	The code has been updated to correctly the free the memory. **Workaround:** None.

92	SBX-108998 | SBX-111014	2	PortFix SBX-108998 to ##9.2.2## - concise view config file is not getting created through REST API. **Impact:** concise view config file is not getting created through REST API. **Root Cause:** Backend API was unable to read username from curl command to append in exportConfig.sh. which was causing the issue. **Steps to Replicate:** Export the concise config file using curl -k -i --user admin:Sonus@123 -X GET 'https://$device_ip:444/pm/api /ImportExport/exportConciseStart' To check the file name, use the below REST API curl -k -i --user admin:Sonus@123 -X GET 'https://$device_ip:444/pm/api /ImportExport/getStatus	Modified code to read username from curl command and added in exportConfig.sh to generate the export directory and exportStatus file. **Workaround**: Need to update ImportExport.php.
93	SBX-110640 | SBX-110916	2	Portfix SBX-110640 to ## 9.2.2 ## - PC 2.0: CDC config not replicated to standby during SWO when there are no active calls. **Impact:** In a PC2.0 setup with HA, when a switch over is performed without LI calls then the interception stops working on the new active. **Root Cause:** The standby SBC is not processing CDC config for realm2hash. Realm2hash is only created if SBC has active LI calls at the time of transition from Active to standby. In case when SBC don't have Active call realm2hash is not created on transition from Active to standby. **Steps to Replicate:** 1. Configure SBC for LI PC2 flavor call. 2. Disabled the peer and realm. 3. Enable peer and realm. 4. Check the realm2hash entry on current active. 5. Perform switch over from active to standby. 6. Check the realm2hash entry on current active.	Standby code is updated to process CDC config and create realm on standby. **Workaround**: Disable/enable CDC Diameter Realm Route and Peer on the new-active.
94	SBX-111162 | SBX-111343	2	Portfix SBX-111162: The SBC fails to defragment/assemble fragmented IPSEC ESP packets received from the customer. **Impact:** The SBC drops an in-coming 1500B IP fragments sent through an IPsec tunnel, where the ESP packet is also fragmented into approximately equal-sized IP fragment packets. This complex IP frag-IPsec-IP frag problem primarily affects large SIP INVITE packets in certain network designs. **Root Cause:** This problem affects large packets sent through IPsec gateways that (1) do no reassemble received IP fragmented packets before sending them through the IPsec tunnel (IP fragments themselves are sent through the tunnel), and (2) fragment resulting ESP packets into approximately equal-sized packets instead of a 1500B and 72B fragments. **Steps to Replicate:** Test should send SIP packets 1500B to SBC over an IPsec tunnel through a device/devices that: 1. Fragments the SIP packet into 1500B + small IP fragments. 2. Sends the IP fragments through the IPsec tunnel. 3. Fragments (again) the larger ESP packet into approximately equal-sized IP fragment packets.	The code is modified to reassemble IP fragments up to 1580B divided any way into a single internal packet buffer, which the IPsec decryption code and subsequent IP frag reassembly code can handle. **Workaround**: Two workarounds are possible: 1. Terminate the IPsec tunnel on a router in front of the SBC instead of directly on the SBC. 2. Do not send the IP fragments through an IPsec tunnel terminated on the SBC. Instead, reassemble IP packets before sending them through the tunnel towards the SBC, so that there is only one level of IP fragmentation (of the ESP packet itself).

Resolved Issues in 09.02.01R003 Release

The following Severity 1 issues are resolved in this release:

Table 25: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution

SBX-107397 | SBX-110861	1	Portfix SBX-107397: There was an SBC switchover DEADLOCK detected for sysID 62, task SIPSG. **Impact:** An SIP call load can trigger a healthcheck timeout in the SIPSG module. **Root Cause:** The problem was with the flags that is used for creation of shared memory between SCM process and fault avalanche handler process. As a result of incorrect setting of flags some of the writes to the shared memory was taking more time resulting in the SCM thread getting blocked and health check timeout. **Steps to Replicate:** 1. Run a 50 cps SIP-SIP call load for an extended period of time. 2. Ensure that the fault avalanche control feature is turned on. "show system faultAvalancheControl facState" should be enabled.	The code is modified to disable fault avalanche control functionality by default. **Workaround:** Disable the Fault Avalance control functionality using the following configuration control. set system faultAvalancheControl facState disabled
SBX-110248	1	The SBC SWe crashes when making a video call with a certain type of phone. **Impact:** The SBC SWe NP crashes when IPsec fragmented signaling packets scenario calls made by using IPsec crypto as NULL encryption. **Root Cause:** During the IPsec crypto null processing of fragments (chained mbuf segments) by the SWe NP, an incorrect first segment length corrupted adjacent buffers, which resulted in a crash of the SBC SWe. **Steps to Replicate:** Establish IPsec session with null encryption and make calls.	The code is modified to address the issue. **Workaround**: Use IPsec non-null encryption suites such AES/3DES.
SBX-111966	1	The SBC/GSX fail to decode trigger response received from the PSX and leads to call failure. **Impact:** Call failures are seen at the SBC when the STI Service is executed for a Trigger Request on the PSX. **Root Cause:** For a two-staged call, the SBC performs a trigger request following an initial policy request to the PSX. If any STI service like signing or verification is executed for this trigger request, the SBC fails to decode a trigger response received from the PSX and leads to a call failure. Compiled diameter Read methods for STI AVPs that are executed on the GSX and SBC are incorrectly looking for TRG_REQ(trigger request) tag while decoding TRG_RESP (trigger response), which is leading to decode errors on the GSX/SBC and resulting in a call failure. **Steps to Replicate:** 1. Perform a two stage call flow with the STI service enabled. 2. Ensure that the SBC sends a trigger request to the PSX for a two stage call call flow and perform the STI service. 3. Observe that there are no diameter decode errors on the SBC that can lead to a call failure.	The code is modified to look for the correct TRG_RESP tag. The SBC builds updates to use new diameter read methods. **Note**: This fix only stops the DIAMETER decoding errors and a further fix is being tracked under another JIRA for a future release to have the SBC pass STI information in the trigger request, as well as process the information in the trigger response to STI service works in conjunction with 2-stage calls. **Workaround:** As a workaround, STI service escapes for a trigger request.

The following Severity 2-3 issues are resolved in this release:

Table 26: Severity 2-3 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-109013 | SBX-110784	2	Portfix SBX-109013: Increase the healthcheck interval. **Impact:** Coredumps are occasionally seen in the field due to the health check timer expiring when the process gets stuck. **Root Cause:** In SWe environments, disk/CPU timing issues can lead to the process slowing down and hitting these health check issues. **Steps to Replicate:** This issue was only reproduced using debug code.	The code is modified to be more forgiving to cope with short spikes. The health check ping interval is now 2 seconds and must have 15 consecutive non responses in order for the process to be declared deadlocked and a coredump initiated to recover. **Workaround**: None.

SBX-109153 | SBX-110776	2	Portfix SBX-109153: DTLS: A 503 Service Unavailable with GCM Ciphers. **Impact:** The following ciphers could not be used with DTLS: 1. ECDHE_RSA_WITH_AES_128_GCM_SHA256 2. ECDHE_RSA_WITH_AES_256_GCM_SHA384 3. RSA_WTIH_AES_128_GCM_SHA256 4. RSA_WITH_AES_256_GCM_SHA384 5. ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 **Root Cause:** The TLS profile had been updated with additional ciphers listed below but the DTLS code was not updated to support these. **Steps to Replicate:** Use aDTLS client that support these ciphers make a connection to the SBC.	The code is modified to include support for these ciphers. **Workaround**: None.
SBX-110205	2	D-SBC: The calling party cannot hear disconnect treatment announcement if M-SBC is a N:1 cluster. **Impact:** The connection IP is not updated when a different M-SBC is selected in clustered D-SBC deployment during disconnect treatment. The SBC was using the old connection IP which was causing the Ingress Peer endpoint not being able to hear the Disconnect Announcement. **Root Cause:** The newly allocated M-SBC media IP during Disconnect Treatment is not used by NRMA due to incorrect validation check and the previous one is used which caused the one way audio issue. **Steps to Replicate:** 1. Configure Disconnect Tone Treatment in the SBC with an M-SBC cluster. 2. From the Ingress endpoint, send SIP INVITE to the SBC. 3. From Egress side send SIP 404 USER NOT FOUND in response to the INVITE. 4. Ensure Ingress side endpoint hears "Disconnect Tone TreatMent".	The code is modified to not use the newly allocated M-SBC media IP during Disconnect Treatment by the NRMA (due to incorrect validation check), and instead use the previous treatment that caused the one-way audio issue. **Workaround**: None.
SBX-110558	3	A call hold from both ends causes a re-INVITE handling issue. **Impact:** Call Holds received from both ends results in a re-INVITE handling issue. **Root Cause:** UserA to UserB call is connected. UserA puts call on hold. Later, UserA triggers a latemedia re-INVITE, and the SBC sends 2xx with offer SDP with a=sendrecv, the local dpm mode changes to sendrecv. The ACK received from UserA with a=inactive. call is still on hold. When userB also initiates the hold (ie., hold from other direction), it should be relayed to UserA. But the SBC not relaying the re-INVITE. Due to improper late media re-INVITE handling, the SBC media state changed, which blocks the relaying of hold re-INVITE from other direction. **Steps to Replicate:** 1. UserA to UserB call is connected. 2. UserA puts call on hold. 3. UserA triggers latemedia re-INVITE, the SBC sends 2xx with offer sdp with a=sendrecv. The ACK received from UserA with a=inactive. 4. UserB sends re-INVITE to put call on hold (ie., hold from other direction). 5. Nothing will be sent to UserA.	The code is modified to relay the hold re-INVITE from the other direction. **Workaround**: None.

Resolved Issues in 09.02.01R002 Release

The following Severity 1 issues are resolved in this release:

Table 27: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-109465 | SBX-109686	1	Portfix SBX-109465: The Leadership algorithm workaround for the openclovis issue can cause a core dump. **Impact:** The safplus_gms process crashes when coming out of split brain. **Root Cause:** Incorrect/inconsistent data results in the code asserting. **Steps to Replicate:** This issue is not easily reproducible and is caused by HA link instability /flapping.	The code is modified so that the data is consistent. **Workaround:** Run HA link stability.

SBX-109893 | SBX-109914	1	Portfix SBX-109893: The SBC frequently switches over with a coredump after 9.2.1R0 upgrade. **Impact:** An SCM core occurred in code that is executed only when the STI feature is enabled. The core was the result of the code in SipSgStiCopyDisplayNametoCPC() attempting to de-reference a NULL pointer. The fix is to add a check for NULL before attempting de-reference the pointer. **Root Cause:** The root cause is that there is code in an STI specific function that attempted to de-reference a NULL pointer. A NULL pointer check is missing in this code. **Steps to Replicate:** Specific steps to reproduce this issue are not known. The root cause and the fix were found by code inspection and core analysis.	The code is modified to check for NULL before attempting de-reference the pointer. **Workaround**: The only known workaround is to disable the STI.

The following Severity 2-3 issues are resolved in this release:

Table 28: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-108469 | SBX-109085	2	A registration issue with a switchover case. **Impact:** Security Mechanism of Registration is set to the TLS in the RCB with two different scenarios. The scenarios are of basic registration, which does not have any security profile. **Root Cause:** Cause is when Reconstruction of RCB happens during switchover by default security is set to TLS without verifying Digest structure. Also whenever the Digest structure is deleted for any reason the code is not setting security back to NONE. **Steps to Replicate:** Test requires a HA setup. Scenario 1: 1. In Active Node make a successful registration. Send a Fake registration such that it gets rejected with 403 error from server side. 2. Now perform a switchover and when standby node becomes active make another fake registration that gets rejected by 403 again. 3. Verify the Security Mechanism in CLI using "show status addressContext default sipActiveRegisterNameStatus" and also try to make a call. Scenario2: (This is for pre-present TLS security before upgrade) 1. In Active node, make a successful registration with response code other than 200 ex: 202 Accepted. [send 202 instead of 200 in server script] 2. Now, send a refresh register, it will be internally rejected with 403 from the SBC. In logs, you will see these statements "invalid state auth-rcvd" and "Refresh register did not meet security requirements". If you verify the security Mechanism it should show TLS. 3. Upgrade the Standby node to 824R2 build. Perform a switchover and send a refresh register to verify the CLI for security mechanism if set to NONE. Try making a call or send a refresh register again both should be successful.	The code is modified so when RCB reconstruction occurs, it verifies the Digest structure whether to set security to TLS or NONE based of the DigestWithoutTLS variable. Whenever the Digest structure is deleted for any reason, the code sets security back to NONE. **Workaround**: Try performing switchover twice.
SBX-109083 | SBX-109820	2	Portfix SBX-109083: The SCM process core dumps during a SipSgAORHashRemove. **Impact:** The SCM Process core dumps due to an entry corruption in the Registration hash table post switchover. This corruption is rare and occurs infrequently. **Root Cause:** The result below is likely to core as a result of the core dump and SYS error logs. The corrupted AOR entry in hash table was allocated during the reconstruction for an Active RCB from standby context after switchover. The SYS Err logs indicate the presence of duplicate AOR entry. This could potential lead to corruption. **Steps to Replicate:** 1. Run a Basic Registration test with switchover. 2. Test with application server sending more than one P-Associated URIs.	The code is modified to ensure that only one AOR entry exists in the hash table after a switchover on the Active SBC's cache. If the AOR entry is not found during remove operation, manually remove the entry to avoid the corruption later. **Workaround**: None.
SBX-107960	2	The AWS IPs remain assigned to the standby SBC, causing unnecessary dual restarts. **Impact:** If the communication between the active and standby is broken (over ha0 interface), both assume active roles (split brain). When this occurs, the standby node that becomes active, calls AWS APIs to move IP address to self. Once ha0 link is restored, the machine, which becomes active, does not call AWS API to move IP addresses, this might cause an issue when the node that has IP does not come up as active, in this case IPs are assigned on standby and another node becomes active. **Root Cause:** The root cause of this issue is not calling a AWS switchover API (move IPs) during split brain recovery. **Steps to Replicate:** Run a split brain test and recovery of SBC HA, and verify that API query is send by the active SBC after recovery.	The code is modified to call AWS APIs to move IP to current active machine during split brain recovery path. **Workaround**: Manually move all secondary IPs to current active machine to restore calls.

SBX-70800 | SBX-109822	2	Portfix SBX-70800: Observing that the metaVariable table is getting modified on loading the backup configuration file of one instance in other instance. **Impact:** When loading the backup configuration from one SBC instance to another, the metavar table is getting populated with the list of metavars from both instances. This alone does not cause any issues so long as the metavars are unique, its just confusing to see the metavars for another instance in the table. **Root Cause:** The code was not removing the existing metavars prior to loading the configuration of another instance. This meant the metavar table had both sets of information. **Steps to Replicate:** 1. Create a backup configuration of one cloud instance (instance1). 2. Loaded the backup configuration file into a new cloud instance (instance2). 3. Check the metaVariables table and see if it contains the metavars from both instances.	The code is modified to flush the metavars for the existing instance prior to loading the configuration from another instance. **Workaround**: None.
SBX-109694 | SBX-109823	3	Portfix SBX-109694: The /node/actualCeName is not updated with new name when there is a change. **Impact:** If a cloud instance is completely rebuilt with a new HA IP value and actualCeName, the new actualCeName is not getting updated into the CDB. The CDB is left with the original actualCeName value. This leads to the SBC being unable to process the new configuration data as it is still trying to read the metavar information based on the original actualCeName value. This in turn leads to the SBC application being unable to start. This problem happens when the textual part of the actualCeName matches but the IP address is different. **Root Cause:** The code was only using the textual part of the name to check if the data in CDB already existed and was not updating the full actualCeName if there was a match on the textual part of the name. **Steps to Replicate:** 1. Rebuilt a cloud instance using the same node name but new IP address and then try to apply this configuration to an instance that is already up and running with the same node name. 2. Check that the SBC application is up and running following the application of the new configuration.	The code is modified to correctly update the actualCeName, even if the node name (textual part of the name) already exists in the CDB. **Workaround**: None.
SBX-108173 | SBX-109685	3	Portfix SBX-108173: The openclovis split-brain recovery data was not always correct. **Impact:** On recovery from split brain, a leader may not be properly chosen, and both machines could stay running for multiple minutes. **Root Cause:** The data passed to the leader election algorithm does not properly indicate that both nodes are leaders. **Steps to Replicate:** Repeatedly break and reconnect the HA connection, checking that the nodes realize they are coming out of split brain (through logs) and one node will properly restart to again become standby.	The code is modified so that the "isLeader" field is properly set and the leader election algorithm can properly detect we are coming out of split brain. **Workaround**: None.

Resolved Issues in 09.02.01R001 Release

The following Severity 1 issues are resolved in this release:

Table 29: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-108557	1	The SBC continuously core dumps for SCM process since upgrade to V09.02.01R000 **Impact:** The SCM Process may coredump due to memory corruption. **Root Cause:** There is code that is using an invalid pointer when writing to a buffer. This code was only added recently in 9.2.1R0. **Steps to Replicate:** This problem is triggered by the receipt of an invalid PDU and/or an SMM rule to reject the incoming Invite and an early ATTEMPT record was attempted to be written. The issue is random and depends on what info is not available when trying to write the accounting record, therefore the issue may not reproduce all the time.	The code is modified to address the issue. **Workaround:** If there is SMM rule (ignore/reject the Invite), then the SMM rule needs to be disabled until patch is applied.

SBX-107690	1	There was call failures observed on T140 load with various MAJOR logs in DBG. **Impact:** Call fails due to RID Enable errors. (where RID = receiver ID and is mapped to an allocated resource) DBG log shows many BrmAsnycnCmdErrHdlr logs with cmd 0x30 (RID Enable): MAJOR .BRM: *BrmAsyncCmdErrHdlr: ERROR NpMediaIntf cmd 0x30 gcid 0x2128915e **Root Cause:** When RTCP Generation is disabled, RTCP RID for the call is expected to be disabled by Network Processor (NP). With introduction of SBX-86241 Streaming RTCP packets to Protect Server, there is now a case where RTCP Generation is enabled to stream RTCP packets to Protect Server but RTCP packets are not generated for the call and RTCP RID for the call is not enabled. When RTCP Generation is disabled NP uses rtcpMode=RTCP Terminate to indicate RTCP RID needs to be disabled. This is incorrect, since rtcpMode=RTCP Relay Monitor also has RTCP RID enabled and NP is expected to disable the RTCP RID. If a call has rtcpMode=RTCP Relay Monitor and RTCP Generation is disabled, leak this particular RTCP RID resource. The next time the particular RTCP RID is allocated, the NP returns an error indicating RTCP RID is already allocated. **Steps to Replicate:** 1. Enable the Packet Service Profile //Resources/profiles/media/packetServiceProfile /rtcpOptions/generateRtcpForT140IfNotReceivedFromOtherLeg. 2. On the SBC, set //System/media/mediaRtcpControl/t140RtcpMonitorInterval to 20 seconds. 3. Start a T140 call but do not send RTCP packet. Terminate the call in 10 seconds. 4. If you keep making this type of call, you will eventually see the Enable RID error. The DBG log will have the BrmAsynCmdErrHdlr entry.	The code is modified so that the BRM indicates the RTCP RID needs to be disabled or not. When the NP receives the command, it uses this new parameter to decide if RTCP RID should be disabled or not. **Workaround**: Disable the RTCP and disable RTCP termination.
SBX-108516	1	A call outage led to DSP errors. **Impact:** The call fails due to the RID Enable errors. The DBG log shows many BrmAsnycnCmdErrHdlr logs with cmd 0x30 (RID Enable): MAJOR .BRM: *BrmAsyncCmdErrHdlr: ERROR NpMediaIntf cmd 0x30 gcid 0x2128915e **Root Cause:** 1. A defect was found in the XRM redundancy processing code where xres->options field was not updated on the standby XRM. 2. When modifying a media flow in NP if RTCP relay monitor is being modified, the XRM did not provide rtcpMode in the media flow modify command. And NP is assuming the RTCP relay monitor is enabled by default. **Steps to Replicate:** Test with calls that use RTCP terminations and will set rtcp-xr-relay-drop to TRUE.	When processing media flow modify request, the code is modified to set the RTCP relay monitor state based on the value in NP_MEDIA_RTCP_REL_MON_STR. **Workaround**: Disable RTCP and RTCP termination in the PSP.

Resolved Issues in 09.02.01R000 Release

The following Severity 1 issue is resolved in this release:

Table 30: Severity 1 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-101155 | SBX-104620	1	Portfix SBX-101155: A DSP coredump occurred on the SBC. **Impact:** The DSP faults with a memory fault in area that pulls buffers out of EMAC port. Suspicion is on buffer size which is reported by EMAC buffer. These errors result in a DSP reload, which is essentially ensures call continuation. Any calls which are using this DSP could have a small media outage while the DSP is reloaded. **Root Cause:** Root cause is a speculation that EMAC system is occasionally is a incorrect bufSize, similar to a bit flip. **Steps to Replicate:** This issue cannot be reproduced, it has been fixed based on code review and coredump backtrace analysis.	The code is modified to look for consistency in packet size and EMAC buffer size reported. In case an inconsistency is found, the packet is rejected, avoiding illegal memory access. **Workaround:** There is no workaround.

SBX-104334 | SBX-106056	1	PortFix SBX-104334: Call Drop when being placed on hold - IPv6. **Impact:** The "anonymous.invalid" in IPv6 media is not considered as as a call hold, and is rejected. **Root Cause:** There is no handling for "anonymous.invalid" while handling calls on hold. **Steps to Replicate:** 1. Establish a normal IPv6 media call. 2. Send a reInvite with "anonymous.invalid" in the c line of the media. 3. Check that the reInvite is not rejected and handled as call hold.	Check for "anonymous.invalid" and if present, consider it as call hold and avoid going for DNS resolution. **Workaround:** Use the SMM to modify "anonymous.invalid" to "::" on the incoming side.
SBX-106452 | SBX-107256	1	PortFix SBX-106452: The Standby SBC SWe on AWS is not coming up. **Impact:** There are hard-coded references to the admin user in SBC LCA code whereby if the admin user is removed, bringing up the SBC may fail on virtual platforms. **Root Cause:** The lack of exception handling to account for admin user usage caused the startup process to error out. **Steps to Replicate:** Create a new Administrator user from CLI/EMA on the Cloud SBC and delete default admin user. Reboot the SBC to check if the SBC comes back up as active or standby.	The code is modified to address the issue. **Workaround:** Follow the MOP: 1. From Active's CLI: Create another Administrator user (e.g. newadmin) CLI commands: set oam localAuth user emsadmin accountRemovalState disabled set oam localAuth user emsadmin passwordAgingState disabled accountAgingState disabled set oam localAuth user newadmin group Administrator 2. From the Active's CLI, delete emsadmin user. CLI commands: delete oam localAuth user emsadmin 3. From shell of both instances, create admin user: Shell command: useradd -p Sonus@123 -G Confd,sftponly,upload, Administrator -s /bin/sh -d /home/sftproot/Administrator /admin admin 4. Reboot the standby instance. 5. Delete the admin user and group from both instances using shell command. Shell commands: userdel admin groupdel admin 6. Login as 'newadmin' user and add 'admin' user CLI commands: set oam localAuth user newadmin accountRemovalState disabled set oam localAuth user newadmin passwordAgingState disabled accountAgingState disabled set oam localAuth user admin group Administrator set oam localAuth user admin passwordLoginSupport disabled passwordAgingState disabled accountAgingState disabled accountRemovalState disabled commit request oam localAuth userStatus admin setRsaKey keyName adminKey rsaKey "<YOUR-PUBLIC-KEY-HERE>" Execute the shell command below on both boxes to reset keep admin user value in cdb. /opt/sonus/sbx/tailf/bin/confd_cmd -o -c "set /SYS:system /admin[0]/sftpUserPassword/keepAdminUser true" 7. Now, the admin user present in /etc/passwd file of both instances.
SBX-105687 | SBX-106176	1	PortFix SBX-106175: An SBC 5400 post upgrade to 9.1, the SMM rule for options stopped working. **Impact:** The SMM rules were not applied after an upgrade to 9.1. **Root Cause:** The logic was modified to pick the same TG for request and response. In the Options ping scenario, request and respond with defaultiptg. **Steps to Replicate:** 1. Upgrade from 8.1 to any later release. 2. Attach the SMM at zone.	The code is modified to address the issue. **Workaround:** NA

SBX-105961 | SBX-106480	1	PortFix SBX-105961: The SBC reInvite with sendonly was causing a one-way audio. **Impact:** The SBC unexpectedly sends out a 'reInvite sendonly' when the relay DPM is disabled. **Root Cause:** Internal logical error to queue the SDP on ingress when egress send 18x (sendonly). **Steps to Replicate:** Enable minimize and disable relay DPM on ingress. A call B, B answer 183 (sendrecv), 183 (sendonly), 183 (sendrecv)...200 (sendrecv)	The code is modified so when subsequent 183 (sendonly) received on egress, the SBC updates the queue sdp (recvonly). Since the relay DPM is disabled, the SBC does not change the direction of datapath on ingress. **Workaround:** n/a. This is an application bug per rfc, and the SDP should not change in subsequent 18x.
SBX-106178 | SBX-106183	1	PortFix SBX-106178: There was a switchover // sonusCpSystemProcessCoredumpGeneratedNotification. **Impact:** The SCM process has cored. **Root Cause:** The SCM has cored when attempting to write a log message because the code is attempting to de-reference a NULL pointer to access information for the log message. **Steps to Replicate:** There are no specific steps for reproducing this issue. This core will only occur in a multi-transfer scenario.	The code is modified to check that the pointer is non-NULL before de-referencing it. **Workaround:** There is no workaround. This core will only occur in a multi-transfer scenario.
SBX-106611 | SBX-107113	1	PortFix SBX-106611: The SBC sends a BYE message within dialog sometimes. **Impact:** After a call is connected, if the SBC triggers internal re-INVITE due to minimizeRelayingOfMediaChangesFromOtherCallLegAll flag on one leg and at the same time. If the SBC receives late media re-INVITE on other leg, the SBC clears the call. **Root Cause:** The internal offer answer state of call at the SBC SIP subsystem becomes invalid. **Steps to Replicate:** Config: minimizeRelayingOfMediaChangesFromOtherCallLegAll enabled. lateMediaSupport -->passthrough E2E Ack Enabled. Egress PSP crypto and SRTP Enabled. Call Flow: Ingress (RTP), Egress (RTP). 1. After call is connected, the SBC triggers internal re-INVITE to egress with one crypto. 2. At the same time , Ingress peer sends late media re-INVITE. 3. LateMedia will get queued up and processed after internal reinvite. 4. But as SBC receives 200OK from egress , it generates 200OK to ingress as a response to late media re-INVITE from ingress. This is wrong. The SBC also sends re-INVITE to egress (late media). Due to this internal state gets messed up and after receiving ACK with SDP from Ingress, the SBC clears up the call. With a fix, verified that the SBC correctly sends 491 Request Pending to ingress when handling internal re-INVITE transaction on egress leg. When the SBC receives another late media re-INVITE on ingress leg , SBC sends it to egress and this second re-INVITE transaction completes successfully.	The code is modified to ensure if the SBC is handling internal re-INVITE on egress leg, late media re-INVITE on ingress leg is responded with 491 Request Pending with RetyAfter header. After the egress re-INVITE transaction is completed, if the ingress peer send another late media re-INVITE it is sent to egress leg correctly and offer answer transaction succeeds for this second re-INVITE. **Workaround:** Suppress the internal re-INVITE on egress leg.
SBX-106691 | SBX-106918	1	PortFix SBX-106691: Adding IPSP fails with the application error. **Impact:** Adding IPSP fails with application error when ipSignalingProfile destinationTrunkGroupOptions is includeDtg, but the error message is not descriptive. **Root Cause:** ERE validates to ensure the check box 'Include DTG' is not selected in the IP signaling profile. The validation was done guiserver but error message was not set and return for why instead of meaningful error message, a very generic error message was coming. **Steps to Replicate:** admin@SBXPLTF1H% set addressContext ADDR_CONTEXT_1 zone ZONE_IAD sipTrunkGroup TG_SIPART_IAD policy signaling ipSignalingProfile AANN [ok][2021-02-02 19:22:08] [edit] admin@SBXPLTF1H% co Aborted: 'sipServiceGroupExt TG_SIPART_IAD ipSignalingProfile': IP Signaling Profile Id 'AANN' cannot be assigned as it is DTG(Destination TrunkGroup) option is selected.	The code is modified to set the error message and and return to provide error message during configurations. **Workaround:** N/A

SBX-106206 | SBX-106710	1	PortFix SBX-106206: An existing hairpin call gets silenced after a switchover. **Impact:** A media loopback is not happening in after switchover. **Root Cause:** There was extra check performed during NP incoming path for the combination of MAC address and loopback flag. **Steps to Replicate:** 1. In the SWe SBC Active-Standby HA setup. 2. Using AS/3GPP call flow scripts/setup establish a call that creates an SBC internal loopback media flow. 3. Verify the media flow and then issue a switchover. 4. Verify the media path on this existing active call.	The code is modified to address the loopback media issue and also saves the NP cpu cycles. **Workaround:** None.
SBX-106968 | SBX-108087	1	PortFix SBX-106968: There was an abnormal switchover on a cluster SBC. **Impact:** The PRS process cored due to accessing NULL destination ICM handle provided by DRM. **Root Cause:** The DRM does not mirror txIcm handle in DRES data structure to standby and the code was not validating the pointer in one specific code path. The code intentionally crashed to identify the bad code. **Steps to Replicate:** The problem could not be reproduced and the solution was found based on code review. There was Edge case timing issues where internal message sent before a switchover and response is processed after a switchover.	The code is modified to validate the tcIcm pointer that is not null before trying to use it and thereby avoids the intentional system error crash. **Workaround:** No workaround
SBX-106722	1	The S-SBC application goes down with a the MESSAGE call load of 11 cps or more. **Impact:** Run the message call flow with the SMM configured with Dialog Scope variables on ingress and egress sides. **Root Cause:** Memory corruption is occuring when we store ingress dialog scope variable id in the Relay CB as it is already freed. **Steps to Replicate:** Run the message call flow with SMM configured with Dialog Scope variables on ingress and egress sides. Run 10 CPS load.	Delaying Relay CB free until we send 200 OK for Message **Workaround:** Disable the Ingress dialog Statefull variable for the SMM rules.
SBX-107586	1	A SAM Process coredump occurred while executing DoS on an SBC SWe SIP signaling port with a malformed Register Message containing 80 multiple unique and spoofed IPs. **Impact:** SIPSG is sending an update to SIPFE for deleting the RCB details with Username, Hostname and PhoneContext as 0 when Register is received with malformed PDU. **Root Cause:** In this malformed Register PDU scenario SIPSG should not send a Delete update to SIPFE. **Steps to Replicate:** Run a load with Register Malformed PDU from IXia or any test tool.	The code is modified for non zero phone context key in SIPSG for sending delete operation update to the SIPFE. **Workaround:** Run in normal mode instead of sensitive mode.
SBX-105764	1	A customer Teams core dump occurred in a TEAMS call flow. **Impact:** A SCM Process core dump resulted for TEAMS call flow. **Root Cause:** Null Pointer exception lead to a SCM Process core dump. **Steps to Replicate:** The steps cannot be reproduced.	The code is modified to prevent the crash. **Workaround:** None.
SBX-107853	1	The SCM process core dump was observed on the standby SBC while running a load with the SBC generated subscribe. **Impact:** The SCm process cores on the standby while running the load for a Reg-Event subscription. **Root Cause:** There is a leak on the standby for SIP dialog data structure, which is causing a SYS_ERROR on the standby. **Steps to Replicate:** 1. Enable the below configuration for Reg-Event feature. set profiles signaling ipSignalingProfile DEFAULT_SIP commonIpAttributes subscriptionPackageSupport supportRegEvent enable 2. Run the load of REGISTRATION for Reg-Event subscription feature.	The code is modified to fix the leak of SIP dialog structure on the standby SBC. **Workaround:** No workaround

SBX-106058	1	Multiple coredumps were observed during a Load run for generated Subscription call Flow tested during Registration Display Enhancement feature. **Impact:** Multiple coredumps were observed when Reg-Event Subscription feature flag gets enabled. **Root Cause:** Core 1: Incorrect type cast of a structure led to invalid memory access and core was observed. Core 2: During a switchover, the list "pendingCcDsIcmList" was never initialized; however, it was incorrectly getting freed. Core 3: Accessing of a NULL pointer led to this core. **Steps to Replicate:** Load test for Reg-Event Subscription initiation.	Core 1: The code is modified to point to valid memory. Core 2: In case of a switchover, the code is modified to initialize the list correctly. Core 3: Before accessing the pointer, the code is modified to resolve the issue. **Workaround:** N/A
SBX-105905 | SBX-106000	1	PortFix SBX-105905: Observed the NP crash during an overload test. **Impact:** Possible memory corruption in NP KNI request queue when KNI requests are not processed in time. **Root Cause:** An older KNI request buffer in the KNI request queue could be concurrently overwritten by a new request while user-space NP logic is still processing it, leading to memory corruption. This issue is more frequent with Mellanox NICs, particularly with multicast mac programming flow. **Steps to Replicate:** Perform an sbxrestart on the SBC with port redundancy enabled, and using a Mellanox-based NIC.	The code is modified to ensure currently handled requests are not overwritten by a new request from the KNI module. **Workaround:** None.
SBX-105269 | SBX-107045	1	PortFix SBX-105269: An SBC crash during a call trransfer produced a coredump. **Impact:** The SCM Process coredumped due to NULL pointer access for a pointer that w as freed due to BYE and HOLD race condition in a transfer call scenario. **Root Cause:** There was an illegal memory access, absence of NULL check, and exposed due to race condition. **Steps to Replicate:** A calls B, B REFERs to C and now A and C talk. After sometime, A sends BYE and C sends re-INVITE with a=inactive at the same time.	The core is modified to address the issue. **Workaround:** None.
SBX-105888 | SBX-106060	1	PortFix SBX-105888: The SBC is sending the wrong TO tag to AS side. **Impact:** The response 200OK for Multi Notify has invalid ToTag. **Root Cause:** Internal logical error when process the 2nd 200OK Notify from AS. The application misinterpretation of the direction of the relay message as IAD. And passing down the wrong data down to SIPS for relaying 200OK to AS. **Steps to Replicate:** IAD Subscribe to AS. the AS sends multiple Notify immediately one after another. The 2nd 200OK of Notify sends to AS has wrong ToTag.	The code is modified so the correct data passes down to the SIPS. **Workaround:** Peer can send 1 Notify at a time. N/A on the SBC.
SBX-108081 | SBX-108199	1	PortFix SBX-108081: Unable to see Video from Cisco 8865/9971 on ConnectMe BYOD client. **Impact:** The SBC drops RTCP packets for video stream if audio stream is transcoded by SBC for a multi-stream call. **Root Cause:** Non-RTCP binding resource was incorrectly picked by the SBC for video stream if audio is transcoded in a multi-stream call. The reason for picking this resource is, natively the SBC did not support audio transcode for a multi-stream call. As a result, the code assumed audio to be in pass-thru mode. **Steps to Replicate:** Configuration: ---------- 1. Configure the SBC for Audio,Video Call. 2. Enable the allowAudioTranscodeForMultiStreamCall in PSP. 3. Enable the rtcp 4. Configure thisLeg and otherLeg, so that audio call will be transcoded. Procedure: ---------- 1. Place an Audio transcoded and Video Relay call through the SBC. Without a Fix: ---------- The SBC drops RTCP packets for video stream. With a Fix: ---------- The SBC relays RTCP packets for video stream.	The code is modified to pick the RTCP binding resource for video stream irrespective of audio being pass-through or transcoded. **Workaround:** Disable the allowAudioTranscodeForMultiStreamCall flag at Route PSP which would result in Audio pass-through call.

SBX-106329 | SBX-106862	1	PortFix SBX-106329: The SBC disconnects a call every few seconds after recovering a DNS server. **Impact:** The SBC disconnects a call every few seconds after recovering a DNS server. **Root Cause:** The DNS client sends a failed lookup response to a DNS agent (SCM ID 03,01 ...) when a probe query fails to get a response for a blacklisted DNS server because a probe query and regular query were used the same FQDN, record type and zone id. The timeout response for probe query in the DNS client process as triggered DNS failed response towards SCM process. **Steps to Replicate:** DNS settings: Three DNS servers are configured. Each weight is set to 50. DNS#1 10.xxx.x.xxx has RRs with ttl=5 DNS#2 10.xxx.x.xxx has RRs with ttl=0 DNS#3 10.xxx.x.xxx has RRs with ttl=0 <Time series> DNS#1 10.xxx.x.xxx process was down (Pkt No.29615). DNS#2 and DNS#3 were available. After few Seconds DNS#2 10.xxx.x.xxx process was down. Only DNS#3 was available.	The code is modified so the DNS probe query does not trigger any response towards a DNS agent from DNS client. So do not send any failure response to the DNS agent in case of probe query failure. **Workaround:** None.
SBX-105439 | SBX-106049	1	PortFix SBX-105439: The SBC does not check if “serverCertName” exists while configuring it as part of the TLS profile. **Impact:** The SBC allows the configuration of the certificate, “serverCertName”, as part of the TLS profile even though that certificate is not present in the SBC. **Root Cause:** The SBC is not validating that a certificate is present during configuration of “serverCertName” as part of TLS profile. **Steps to Replicate:** Verify the SBC does not configure a certificate which is not installed. Steps to verify issue: 1. Bring up the instance. 2. Configure the certificate that is not present in the below path. show system security pki certificate. set profiles security tlsProfile defaultTlsProfile serverCertName <Name> Expected result: The SBC does not allow configuring “serverCertName” as part of the TLS profile. Steps to verify fix: 1. Bring up the instance. 2. Configure certificate that is present in the below path. show system security pki certificate. set profiles security tlsProfile defaultTlsProfile serverCertName <Name> Expected result: The SBC allows configuring “serverCertName” as part of the TLS profile.	The code is modified for the SBC to validate whether a certificate being configured is present or not on the SBC. **Workaround:** None.
SBX-106224 | SBX-106481	1	PortFix SBX-106224: An SBC failover with the SCM process core dumps due to memory corruption. **Impact:** When Prack is enabled on the ingress and advanced SMM for "variableScopeValue message" is enable, the SBC may core when the egress responds with 18x/2xx in quick succession, and the Prack is still pending. **Root Cause:** When 18x/2xx is queuing on the ingress, the SBC did not allocate proper resources for "variableScope" data. By the time the SBC sends the data out, it accesses invalid data. **Steps to Replicate:** This is random issue that is not easily reproducible. 1. Egress: inbound config variableScopeValue message and send to ingress. For example: store "*99" in var1. 2. Ingress: prack enable, outbound read the var1 and append to the userName of To Header. 3. Egress: send multiple 18x/200 fast to trigger some delay on ingress for sending. 4. Run a load.	The code is modified to properly allocate resource for "variableScope" data. **Workaround:** Disable prack.

SBX-106476 | SBX-107115	1	PortFix SBX-106476: The ipAdaptiveTaransparencyProfile is not working for a re-INVITE coming from Egress. **Impact:** When the sipAdaptiveTransparencyProfile is configured for Egress TG and re-INVITE comes from egress peer with change in P-ASSERTED-ID, the SBC does not relay the invite from egress to ingress. **Root Cause:** The SBC code does not set service bit for reINVITE transparency for re-INVITEs coming from egress peer. **Steps to Replicate:** Test case 1. Configure the sipAdaptiveTransparencyProfile for Egress TG for re-INVITE. config set profiles services sipAdaptiveTransparencyProfile ADP2 sipMethod INVITE triggerHeader P-ASSERTED-ID action new-value trigger value-change set profiles services sipAdaptiveTransparencyProfile ADP2 state enabled set addressContext ADDR_CONTEXT_1 zone ZONE4 sipTrunkGroup SBXSUS7_LABSIP2 services sipAdaptiveTransparencyProfile ADP2 commit When egress sends a re-INVITE with modified PAI after call is connected, no re-INVITE is generated towards the ingress side. Test case 2 Verify the issue. With a fix, the re-INVITE is relayed to ingress for both late and early media cases.	The code is modified to ensure the SBC sets the service bit for egress properly when the sipAdaptiveTransparencyProfile is configured for egress TG. **Workaround:** None.
SBX-106920 | SBX-107730	1	PortFix SBX-106920: The FmMasterProcess dumped core after a switchover with stable call. **Impact:** The FmMasterProcess core dumps during shutdown. **Root Cause:** The FmMasterProcess may deadlock during shutdown due to receiving an event while trying to shutdown/finalize the event handling. **Steps to Replicate:** This is extremely time-sensitive and requires publishing an event from AMF to FM at just the right time in the shutdown sequence. There is no way to consciously reproduce the issue.	The code is modified to avoid the possibility of the deadlock. **Workaround:** No workaround.
SBX-107041 | SBX-107802	1	PortFix SBX-107041: The OAM and MRFP goes down due to component error time reset for SsreqProcess,SLwredProcess, and when the FmMasterProcess is going down. **Impact:** The OAM and MRFP goes down due to component error time reset. **Root Cause:** The NTP is not synced before the SBC comes up. As a result, when the sync occurs after the SBC comes up and the new time is older than the current time, the SBC goes down. **Steps to Replicate:** 1. Launch the SBC with a time zone and the NTP in sbx.conf. 2. Check if the NTP server was properly synced and there was no issue of "time getting reset to past" in the SBC logs.	Run NTP sync operations before starting serf to avoid any issue when the time sync occurs and time gets reset to past. **Workaround:** No workaround.
SBX-106732	1	The CE_Node1.log is filling up quickly. **Impact:** The CE_Node1.log file size grows to an excessive size cauing a hard disk space alarm. **Root Cause:** An excessive number of log prints were coming from stack trace dumps on a SYS_ERR (EVLOG). **Steps to Replicate:** Run a suite of REFER call scenarios and see that NrmaCpcCallVerifyTimerFunc is not being written in CE_Node log.	Converted the SYS_ERR(EVLOG) event for the concerned log event to NrmaDlog, so the CE_Node.log file no longer contains the back trace. **Workaround:** echo > CE_Node.log when it grows too big.
SBX-107439	1	The SWe_NP - KNI was out of memory **Impact:** On the Azure platform with Mellanox ConnectX-3 accelerated NICs, the packet port interfaces may lose connectivity. **Root Cause:** The buffer pool associated with Packet interfaces was getting exhausted due to lazy free logic in DPDK's driver for Mellanox ConnectX-3 NIC. **Steps to Replicate:** Route few calls to the same packet interface as incoming and some calls to the other packet interface.	The code is modified in order to alleviate stress on the buffer pool. **Workaround:** None.

SBX-107397	1	After an SBC switchover, a DEADLOCK was detected for sysID 62, task SIPSG. **Impact:** The SIP call load can trigger healthcheck timeout in SIPSG module. **Root Cause:** The problem was with the flags that is used for creation of shared memory between SCM process and Fault Avalanche handler process. As a result of incorrect setting of flags, some of the writes to the shared memory was taking more time resulting in the SCM thread getting blocked and health check timeout. **Steps to Replicate:** 1. Run a 50 cps SIP-SIP call load for an extended period of time. 2. Make sure that the fault avalanche control feature is turned on. "show system faultAvalancheControl facState" should be enabled.	The code is modified to disable Fault Avalanche control functionality by default. **Workaround**: Disable the Fault Avalance control functionality using the following configuration control: set system faultAvalancheControl facState disabled

The following Severity 2-3 issues are resolved in this release:

Table 31: Severity 2-3 Resolved Issues

Issue ID	Sev	Problem Description	Resolution
SBX-106815 | SBX-107963	2	PortFix SBX-106815: The PES process was leaking memory. **Impact:** In certain circumstance with high enough call rate, the SBC may experience PES memory leak. **Root Cause:** The newly ported Postgres code mishandled Postgres DATABASE cursor and counter. **Steps to Replicate:** This problem has been fund and reproduced in Comcast lab, when they were testing their call load.	The colde is modified in cursor and counter area. **Workaround:** Lower call rate should lower the risk.
SBX-107593 | SBX-107595	2	PortFix SBX-107593: There is DTLS support for version 1.2. **Impact:** The SBC did not support DTLS clients which only supported DTLS version 1.2 to connect. **Root Cause:** The SBC was hardcoded to only support DTLS version 1.0. **Steps to Replicate:** Make a call from the DTLS client that only supports DTLS version 1.2 and check that the SBC is able to establish the call.	The code is modified to allow support for up to DTLS version 1.2. **Workaround:** None.
SBX-105483 | SBX-105739	2	PortFix SBX-105483: There was a malformed P-charging vector. **Impact:** P-Charging-Vector was not passed transparently to egress on SIP-I to SIP call, when Create P-Charging-Vector is selected on egress IP profile and Store P-Charging vector is selected on ingress IP profile. **Root Cause:** The SIP-I INVITE contains IAM with a bad parameter and no parameter compatibility, causing the SBC to send 183 with CFN message and not transit the P-Charging-Vector. **Steps to Replicate:** 1. Make SIP-I to SIP call. 2. SIP-I IAM contains an unrecognized parameter with no parameter compatibility information. 3. Ingress IP profile has Store P-Charging-Vector. 4. Egress IP profile has Create P-Charging-Vector.	Correct code to ensure P-Charging-Vector is passed to egress in this case **Workaround:** Disable support for the CFN message in ISUP signaling profile.
SBX-105674 | SBX-105892	2	PortFix SBX-105674: Turk Telecom coverity issues part2. **Impact:** While processing SUBSCRIBE messages the coverity tool has highlighted that the code could dereference a pointer that is potentially null. Although no bad behaviour has been observed during testing there is a small chance that it could result in coredumps if the pointer really was null. **Root Cause:** Based on other validation in the code coverity highlighted that some legs of code could result in accessing a pointer that might be null. Derefencing null pointers can cause unexpected behaviour and in the worst case coredumps. **Steps to Replicate:** Run various SUBSCRIBE related test cases.	The code is modified to validate that the pointer is not null before using it to avoid any potential issues/coredumps. **Workaround:** None.
SBX-105497 | SBX-107250	2	PortFix SBX-105497: The wrong format of the SIP 400 BAD REQUEST. **Impact:** When the SBC received a message that is unable to find the required headers, the SBC responses 400 with syntax errors itself. **Root Cause:** The peer intentional sending garbage message. **Steps to Replicate:** Incoming request with have required headers as part of content body section.	The code is modified so the SBC discards the message. **Workaround:** Use the SMM to drop the message.

SBX-102277 | SBX-106516	2	PortFix SBX-102277: The debug command caused ScmP to coredump **Impact:** We are hitting a Healthcheck timeout when displaying the output of the following debug command: "request sbx sipsg debug command "svcgrp -ce 0 -scm <x> -1"" **Root Cause:** The Heathcheck timeout is because it is taking too long to display the data for all of the service groups when there are very large number of trunk groups configured. **Steps to Replicate:** 1. Configure the 1000 TGs 2. Issue the following command: "request sbx sipsg debug command "svcgrp -ce 0 -scm <x> -1""	The code is modified to only display up to 50 service groups in order to prevent this Healthcheck timeout. **Workaround:** To prevent this issue: Avoid using the following command if there are large number of TGs configured: "request sbx sipsg debug command "svcgrp -ce 0 -scm <x> -1""
SBX-105160 | SBX-107902	2	PortFix SBX-105160: There was a CHM process coredump on standby OAM after reboot. **Impact:** The SBC application continues to come up even when asp.py zap (zapAsp() call in sbxCleanup.sh) is invoked from sbxCleanup.sh script. When we try to access ceNum in one of the places, since it is not properly set due to failure in sbxCleanup.sh, it results in CHM coredump **Root Cause:** The SBC application continues to come up even when asp zap is called. **Steps to Replicate:** Fail sbxcleanup in one of the places and ensure the SBC in not being brought up.	The code is modified to avoid the SBC bring up if any errors are reported in sbxCleanup. **Workaround:** The issue is fixed, no workaround is required.
CHOR-7376 | SBX-107023	2	PortFix CHOR-7376: There was a Swe_UxPad coredump observed during Teams Testing. **Impact:** The SWe_UXPAD process crashes due to the health check failure in extra-low memory SWe configuration on Microsoft Azure with presence of outgoing STUND/DTLS traffic. **Root Cause:** The root cause was identified to exhaustion of an internal buffer pool during the presence of STUN/DTLS traffic. **Steps to Replicate:** Launch a 6GB SWe instance in azure using accelerated NIC. Run a Teams test suite for multiple iterations which would trigger STUN/DTLS traffic to go out from SWe.	The code is modified to adjust the internal buffer pool size in order to account for additional requirements of STUN/DTLS traffic. **Workaround:** No workaround.
SBX-107420 | SBX-107880	2	PortFix SBX-107420: Failed to download the Call Diagnostics file. **Impact:** Unable to download a large size call diagnostics log file. **Root Cause:** When we tried to download a large size call diagnostics log file. It was failing with JAVA heap error because IOUtils toByteArray API was created internally ByteArrayStream to store file data into byte format. Due to java memory restriction, we were getting a Heap error from ByteArrayStream. **Steps to Replicate:** Steps to reproduce the issue: 1. Login into EMA. 2. **Troubleshooting** > **Troubleshooting Tools** > **Call Diagnostics**. 3. Click on Save Call Diagnostics button to generate the log file. 4. Go to the Call Diagnostics Data Files section and try to download the tar file. 5. If the file size is more than 400MB, it should get failed with a proxy error.	The code is modified to internally copies the data from inputStream into OutputStream. **Workaround:** NA
SBX-105290 | SBX-108092	2	PortFix SBX-105290: The SBC CDR: Redirecting digits captured incorrectly. **Impact:** The redirecting number recorded in the CDR was not correct if the first policy dip route was used for the call but there was an updated redirecting number from a later route in the policy dip. **Root Cause:** The code was incorrectly using the last per route redirecting number from the policy response to overwrite the redirecting number from the received INVITE message and using this to populated the redirection information field in the CDR record. **Steps to Replicate:** Configure the PSX routing label with two different route with two different ingress trunkgroups, and in each trunk add a DM rule for RDN. Now, make a call check what is the RDN from the CDR logs. If the call gets success with route 1 then it should have RDN according to DM rule in route1. The variations in tests: Test1 => route1 has DM/PM rule to remove CC in RDN and OCN, route 2 has DM/PM rule to modify RDN and OCN. CALL SUCCESS with Route1 TEST2 => route1 has DM/PM rule to remove CC in OCN No rule for RDN, route 2 has DM/PM rule to modify RDN and OCN. CALL SUCCESS with Route1 TEST3 => route1 has DM/PM rule to remove CC in RDN No rule for OCN, route 2 has DM/PM rule to modify RDN and OCN. CALL SUCCESS with Route1	The code is modified to populate the CDR using the per route redirecting number digits or the contain received from the INVITE. **Workaround:** Not Applicable.
SBX-105901 | SBX-106712	2	PortFix SBX-105901: There is a heap-buffer-overflow in the ASAN build for SIPS module. **Impact:** Observing the heap buffer overflow in SCM process for info level log while decrypting the ROUTE header. Reading memory beyond the end of the allocated buffer can result in memory access faults and coredumps. **Root Cause:** A heap overflow occurs because the debug statement is trying to print from a string variable that is not null terminated. **Steps to Replicate:** Execute a test case where INVITE message contains encrypted route-header and verify that there are no failures.	The code is modified to create a local variable of type character array, which gets dynamically created and is always null terminated. This variable is used in the info log. **Workaround:** Not Applicable.

SBX-103183 | SBX-106171	2	PortFix SBX-103183: The SBC incorrectly formatted the rport in the VIA header. **Impact:** The SBC incorrectly formats the rport value in the header of the response message when rport has a valid port number and is at the end of VIA header of request message. **Root Cause:** The code does not verify that rport has a valid port number. If rport is the last parameter in VIA header, the SBC appends "=<source port>". **Steps to Replicate:** 1. Setup: SIPp - SBX - SIPp 2. Send Register message with "rport=1111" in VIA header from client SIPp script with to the SBC. "rport" is at the end of VIA header 3. Run the client script with -p 30333 4. Verify that the SBC replaces rport port number (1111) with its own rport (30333) in VIA header of 200 OK response.	The code is modified so that it checks for any port number in rport parameter (rport is at the end of through the header of request message), it replaces the port number and appends it's own rport. **Workaround:** Use the following SMM as a workaround: set profiles signaling sipAdaptorProfile HeaderModifications rule 1 applyMatchHeader one set profiles signaling sipAdaptorProfile HeaderModifications rule 1 criterion 1 type message message messageTypes response statusCode 200 set profiles signaling sipAdaptorProfile HeaderModifications rule 1 criterion 2 type header header name Via condition exist set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 type header operation store set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 headerInfo headerValue set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 from type header value Via set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 to type variable variableValue var4 set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 2 type variable operation regsub set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 2 from type value value "rport=" set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 2 to type variable variableValue var4 set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 2 regexp string "rport=[0-9]*=" matchInstance one set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 3 type header headerInfo headerValue set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 3 operation modify set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 3 from type variable variableValue var4 set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 3 to type header value Via

SBX-104975 | SBX-106101	2	PortFix SBX-104975: The MCF id sent back to the ingress as MPS during T.38 Fax to G.711 transmission. **Impact:** Some fax T.38 endpoints send an entire DCS V.21 signal in one packet as opposed to 1 octet per packet. This can causes fax failures. **Root Cause:** A burst of octets in a single packet is essentially a burst, and causes potential problems as these packets get queued for modulation and cause delay and later TCF (high speed) signal some packets get dropped. **Steps to Replicate:** Refer to unit test description in the JIRA.	The code is modified to accommodate such larger bursts. **Workaround:** This bug is a specific interoperability problem with such endpoints which exhibit burst single packet DCS signals. For such endpoints, a workaround is not available unless some configurations are available on those devices to modify this behavior.
SBX-106269 | SBX-106800	2	PortFix SBX-106269: RTT-TTY uppercase behavior is inconsistent. **Impact:** Sometimes ASCII letters received in a T140 packet are sent as numbers and figures characters on g711 baudot side. **Root Cause:** Baudot has two modes - LTRS mode and FIGS mode. After transmitting 72 characters continuously in one mode, the recommendation requires to repeat LTRS or FIGS baudot tone to reassert the current mode. LTRS and FIGS mode have some common baudot codes such as 0 (BKSP),2(LF), 4(SPACE) and 8 (CR). There is no need to change mode when any of these common characters need to be transmitted. The issue is that when in LTRS mode 72nd character is received as one of common characters mentioned above, then the SBC incorrectly sends FIGS mode baudot tone. As a result, all subsequent LTRS characters are interpreted as FIGS and show incorrectly on screen of receiving phone **Steps to Replicate:** Create a t140 pcap with characters in each packet (per line) such as this. Note there is LF character after each line.	After 72 characters of same mode (LTRS or FIGS) the stack sends LTRS/FIGS baudot code. If 72nd characters is common code such as BKSP, SPACE, CR or LF and the if previous mode was LTRS, stack sends FIGS baudot tone. Fix to check current LTRS/FIGSmode and send the LTRS/FIGS baudot code. **Workaround:** There is no workaround as such.

AAAAAAAA
BBBBBBBB
CCCCCCCC
DDDDDDDD
EEEEEEEE
FFFFFFFF
GGGGGGGG
HHHHHHHH
00000000
11111111
BBBBBBBB
CCCCCCCC
DDDDDDDD
EEEEEEEE
FFFFFFFF
GGGGGGGG
HHHHHHHH
IIIIIIII
AAAAAAAA
BBBBBBBB
CCCCCCCC
DDDDDDDD
EEEEEEEE
FFFFFFFF
GGGGGGGG
HHHHHHHH
IIIIIIII
AAAAAAAA
BBBBBBBB
CCCCCCCC
DDDDDDDD
EEEEEEEE
FFFFFFFF
GGGGGGGG
HHHHHHHH
IIIIIIII

Before the fix, the following appeared on g711 baudot side:
AAAAAAAA
BBBBBBBB
CCCCCCCC
DDDDDDDD
EEEEEEEE
FFFFFFFF
GGGGGGGG
HHHHHHHH
00000000
11111111
BBBBBBBB
CCCCCCCC
DDDDDDDD
EEEEEEEE
FFFFFFFF
GGGGGGGG
HHHHHHHH
IIIIIIII

????????
::::::::
$$$$$$$$
33333333
!!!!!!!!
++++++++
========
88888888

????????
::::::::
$$$$$$$$
33333333
!!!!!!!!
++++++++
========
88888888

After fix the T140 characters are displayed correctly.

SBX-106822 | SBX-107399	2	PortFix SBX-106822: There was a crash observed in Four GPU Codec Scenario. **Impact:** The G.729AB GPU codec may crash when packets are lost in the incoming G.729AB stream which, in turn, leads to SWe_UXPAD crash and an SBC application restart. **Root Cause:** An uninitialized stack variable in GPU G.729AB decoder code was identified as the root cause. **Steps to Replicate:** 1. Set sweActiveProfile to use GPU, and sweCodecMixProfile to use G.729. 2. Make a G.729AB to G.711U call, and don't send the media. RESULT: SWe_UXPAD may crash and the SBC application restarts. **NOTE**: The issue is not always reproducible.	The code is modified to initialize the stack variable appropriately. **Workaround:** No workaround.
SBX-105413 | SBX-105956	2	PortFix SBX-105413: Support for 3072-bit long RSA keys is missing. **Impact:** The SBC needs to support 3072-bit RSA keys in certificates. **Root Cause:** A feature change is required to support 3072-bit RSA keys in certificates in addition to 2048-bit and 4096-bit RSA keys. **Steps to Replicate:** 1. Test 3072-bit RSA key certificate on client. Make SIP-TLS call from the client to the SBC acting as TLS server. 2. Configure remote certificates with 3072-bit RSA key. 3. Configure local certificates with 3072-bit RSA key. 4. Test 3072-bit RSA key certificate on SBC acting as SIP-TLS server.	The code is modified to provide support for 3072-bit RSA keys in certificates. **Workaround:** None.
SBX-106149 | SBX-106641	2	PortFix SBX-106149: The PSP QoS non-zero value of msrpDscp cause PES to crash. **Impact:** The PES process crashes when apps starting up if msrpDscp in PSP QoS values configured with non-zero. **Root Cause:** A debug statement tried to print a integer as a string, causing memory problem. **Steps to Replicate:** 1. Configure the non-zero msrpDscp value. 2. Restart the SBC. Before the code change, the PES will crash. After the code change, the PES will not crash.	The code is modified to print integer as integer. **Workaround:** Do not configure a non zero msrpDscp.
SBX-107348 | SBX-107360	2	PortFix SBX-107348: The SIP LM call re-Invite sent in the 18x-PRACK stage on ingress. **Impact:** The SBC sends a reInvite to the late media while the call is still in prack pending state. **Root Cause:** Logical error that fail to detect the state of call not connect yet and the SBC tries to send the reInvite out. **Steps to Replicate:** 1. Configure the LRBT. 2. Incoming late media with prack support. 3. Egress 180 trigger play tone, 180 again again, and 200OK(sdp). 4. Ingress delay sending prack for 5secs.	The code is modified to validate the state of the call before reInvite out. **Workaround:** Disable prack or disable LRBT.
SBX-104113 | SBX-105070	2	PortFix SBX-104113: The mediationServer signaling channel was online even interface went down. **Impact:** Without this fix, the LI - mediationServer signaling channel stays online even after ipInterfacegroup attached to call data channel(CDC) is disabled post a switch-over. **Root Cause:** The SBC code, handling the LI - mediation server signalling socket functionality did not register for ipInterfaceGroup operational status in standby mode. As a result, post switch-over it does not get any notification when ipInterfaceGroup attached to CDC toggles. The signaling connection towards mediation server is not closed. **Steps to Replicate:** 1. Create CDC and configure it for IMSLI and validate that the LI signaling channel is inService. 2. Perform a switch-over. 3. Disable the ipInterfaceGroup attached to the CDC.	The code is modified to register for the ipInterfaceGroup that is attached in CDC in standby mode as well so that if and once it becomes active due to switch-over it would get operational status of the ipInterfaceGroup attached to CDC. **Workaround:** N/A

SBX-105711 | SBX-105924	2	PortFix SBX-105711: There was a ASAN MRFP: CE_2N_Comp_CpxAppProc leak during disable and enable of pkt port **Impact:** Creating an H248 signaling port results in a small memory leak. **Root Cause:** While processing the H248 signaling port creation command when metavars are defined for the IP value, the SBC allocated memory to hold the metavar value from CDB internally for processing, but never freed up this memory block at the end of the port creation action resulting in a small leak. **Steps to Replicate:** Create an MRFP instance where metavars are used to define the IP value for the H248 signaling port.	The code is modified to correctly free the memory block at the end of processing the signaling port creation. **Workaround:** None.
SBX-103306 | SBX-107647	2	PortFix SBX-103306: Allocated bandwidth for opus call is 1032kb and 1028kb for single call. **Impact:** If "transcoderFreeTransparency(TFT)" is enabled at Route PSP, then extra bandwidth is allocated for opus call in case maxaveragebitrate attribute is not received in SDP from the endpoints. **Root Cause:** If maxaveragebitrate is not received in SDP, then the SBC was using the max value of 510kbps as the default value (which was not as per RFC). Later, this bitrate value gets intersected with Route PSP configured value. However, for TFT calls, this intersection with route PSP does not happen. As a result, the SBC continues to maintain this value as 510kpbs, which results in extra bandwidth allocation. **Steps to Replicate:** Configuration: 1. set profiles media packetServiceProfile DEFAULT packetToPacketControl transcode transcoderFreeTransparency 2. set profiles media packetServiceProfile DEFAULT secureRtpRtcp flags enableSrtp enable allowFallback enable (Ingress) To re-create the issue: 1. UAC sends INVITE with OPUS codec and SDP does not contain "maxaveragebitrate" attribute. 2. Since "maxaveragebitrate" is not received from UAC, the SBC defaults to max value of 510kbps and sends the same to UAS. 3. UAS responds 200OK with OPUS codec and SDP does not contain "maxaveragebitrate". 4. The SBC sends out 200OK with maxaveragebitrate=510kbps to UAC. Test Result without a fix: Since maxaveragebitrate defaults to 510kbs, the SBC ends up allocating more bandwidth than expected.	If "maxaveragebitrate" is not received in SDP, then derive the default value according to RFC using "maxPlayBackRate" and mode(mono /stereo). **Workaround:** None.
SBX-107611 | SBX-107612	3	PortFix SBX-107611: The AMRWB bit-exactness problem in case of mixed mode test. **Impact:** Degraded audio in AMRWB stream when AMRWB (GPU) call load is running, particularly when each call uses different mode. **Root Cause:** Root cause was identified to an issue with context rearrangement code of GPU AMRWB codec. **Steps to Replicate:** 1. Set sweActiveProfile to use GPU and sweCodecMixProfile to use AMRWB. 2. Make AMRWB to G711U call load using multiple AMRWB clients, each client using different mode. RESULT: Some of the calls may have degraded audio in AMRWB stream.	The code is modified to address the issue. **Workaround:** No workaround.
SBX-107924 | SBX-107931	2	PortFix SBX-107924: The OAM services are not coming up with 6GB Ram with network interface mapping error. **Impact:** The SWe_NP process fails to come up in a 6GB OAM instance configured with only 2 interfaces (ha0 and mgt0). **Root Cause:** Lack of sufficient huge pages in this particular scenario causes SWe_NP initialization failure. **Steps to Replicate:** Bring up a OAM node with 6GB RAM instance and configure two interfaces (without any pkt interfaces). The OAM instance would fail to come up.	The code is modified to reserve enough huge pages required for SWe_NP. **Workaround:** Configure OAM instance with >= 16GB. This is the officially supported configuration for OAM instance.

SBX-60855 | SBX-106922	2	PortFix SBX-60855: The OPTIMA FTTH Stat for TG-A and TG-C Stat mismatching. **Impact:** The active register count on ingress TG is not decremented when a bad refresh REGISTER is received. Due to this there is difference in count of total stable registrations across zones. **Root Cause:** When the load of bad Refresh or initial REGISTERs received, at SBC for some of the registers not getting userNPhoneContextKey due to this the code that is responsible for reducing activeRegCount is not executed. **Steps to Replicate:** 1. First make one active Registration. 2. After active registration send one bad refresh REGISTER. Expected Result: After bad refresh REGISTER, the SBC sends 400 Bad to Refresh REGISTER and also reduces the activeRegCount on ingress Side but it will not reduce count on egress side,	The code is modified to address the issue. **Workaround:** None.
SBX-102700 | SBX-106306	2	PortFix SBX-102700: The number mapping (translated, RDI, To hdr, R-URI) is unexpected. **Impact:** The SBC is not adding translated number received from PSX to RequestURI when Diversion header is present in the ingress Invite. **Root Cause:** If the ingress Invite does not contain Diversion header, then the SBC is adding translated number to RURI. So same result is expected when diversion header is present. **Steps to Replicate:** 1. Make a SIP call by sending an Invite with Diversion header from UAC. 2. Configure PSX to return "translated number" for the called party number in policy response. 3. The SBC includes the translated number in Request URI and routes the call.	The fix is to populate the RequestURI with the translated number even when the Diversion header is present in the initial Invite. **Workaround:** None.
SBX-104507 | SBX-106552	2	PortFix SBX-104507: The SBC is not passing URI parameter while History to Diversion interworking **Impact:** The SBC is not passing URI parameter "user=phone" while interworking History-Info header to Diversion header. **Root Cause:** The SBC was not adding "user=phone" during interworking History-Info header to Diversion header for the SIP uri. **Steps to Replicate:** 1. On the ingress leg, enable acceptHistoryInfo. 2. On the egress leg, enable diversionHistoryInfoInterworking. 3. Run a basic call with History-Info header having SIP uri and "user=phone" parameter.	The code is modified to add "user=phone" during interworking History-Info header to Diversion header for the SIP uri. **Workaround:** None.
SBX-106042 | SBX-108135	2	PortFix SBX-106042: The RCB(s) can be hijacked and effect on registered users/EPs. **Impact:** Issue 1: When the register is sent to the registrar, the SBC creates a RCB for that particular User. When a fake/hijacked register is rejected with 403, some of the parameters in RCB are being modified and users were unable to make a call due to security mechanism being set to TLS. Issue 2: If a timeout on the RCB leads to it moving to a terminated state and a refresh register arrives, subsequent calls are rejected. **Root Cause:** Issue 1: When a Register request is rejected with a 403, it moves to the terminated state. Also, when a register is received, the RCB details are modified irrespective fo the response received from the registrar. **Note**: A register is considered fake when we receive a 403 response for that. Issue 2: When the RCB was moved to the terminated state, the code was partially deleting internal memory that led to reporting the RCB mechanism as TLS, and not rejecting the TLS calls. **Steps to Replicate:** Use the conas mentioned in the description and use the config file attached for reference: 1. After config make a successful registration, later make a register so that it gets rejected with 403 error. 2. Verify the parameters in RCB using this command: show status addressContext default sipActiveRegisterNameStatus 3. Check for all the displayed parameters and also check for sipSigPort and other essential parameters in Debug logs.	The code is modified for: 1. When we receive a fake register and 403 response the RCB should remain in previous state with the previous information. The RCB contents are backed up so they can be restored on failure. 2. Remove the security mechanism of TLS when the RCB is in terminated state. **Workaround:** No Workaround.

SBX-102726 | SBX-106883	2	PortFix SBX-102726: The Diameter RX had the wrong data in media-component AVP post T.38-488. **Impact:** Sending the wrong data in media-component AVP (codec-data) when T.38 failback fails. **Root Cause:** Instead of sending last negotiated codec, the SBC was sending previous offer-answer data in the media-component AVP of AAR message. **Steps to Replicate:** 1. Configure PSPs for faxfallback and enable Rx feature. 2. Run transcode call (A(PCMA) and B(PCMU)). 3. The B sends fax tone, on detecting fax tone the SBC sends T.38 Re-INVITE towards A and A rejects with 488. 4. When a fallback happens, the SBC sends G711 Re-INVITE towards A and gets 200 OK. On getting 200 OK. The SBC sends final AAR that should contain last negotiated SDP information.	The code is modified to address the issue. **Workaround:** Not Applicable.
SBX-105450 | SBX-106573	2	PortFix SBX-105450: A failure to delete remote server configured with FQDN for multiple commits. **Impact:** Failure to delete remote server configured with FQDN for multiple commits. **Root Cause:** The confd iter stops on returning failure for not finding any child remote servers for the first remote server and we fail to process the delete request for the second remote server that leaves the child remote servers of the second remote server as is. **Steps to Replicate:** 1. Configure multiple FQDN remote servers such that first server fails to resolve FQDN and the second server creates child remote servers. 2. Disable both the remote servers. 3. Delete the first remote server and then the second in a single commit. 4. The remote servers created by second remote server fails to delete.	Return success from delete remote server function so that next CDB operation is processed. Failure to find a server is anyways logged and is not shown on the CLI as an error. **Workaround:** Delete the remote servers in separate commits.
SBX-106913 | SBX-107027	2	PortFix SBX-106913: There was a SCM process coredump for register with timeout from Application server with no response. **Impact:** The coredump observed when the SBC logs account info incase of register timeout. **Root Cause:** There was a NULL check miss in the code so coredump observed when we try to access account information. **Steps to Replicate:** 1. Send a REGISTER from UAC, the SBC sends towards AS. 2. The AS sends 302 to REGISTER. 3. The SBC sends redirected REGISTER to next AS and tries for 5 times since there is reply from AS.	The code is modified to address the issue. **Workaround:** Not applicable.
SBX-105050 | SBX-105675	2	PortFix SBX-105050: The SBC DRBD mount not visible on active the SBC. **Impact:** The SBC DRBD mount was not visible on the active SBC. **Root Cause:** When the sbxrestart is issued from platform manager, DRBD gets mounted on apache's mountspace. **Steps to Replicate:** 1. Bring up both the nodes. 2. Do an SBC restart from pm on active. 3. The new active must have drbd mounted.	Modify the apache service file and set the resposible parameter (PrivateTmp) to false. **Workaround:** None.
SBX-105736 | SBX-106560	2	PortFix SBX-105736: Sending the m=application 0 UDP/BFCP (null) in case of UPDATE. **Impact:** The SBC sends m=application line in incorrect format in SIP UPDATE message. **Root Cause:** The SBC does not format m=application line for UDP/BFCP when sending UPDATE message. **Steps to Replicate:** Test case 1. Reproduce the issue. The SBC sends a INVITE with SDP(with audio and video lines and m=application) and receives rel 18x with SDP(with audio and video lines only) followed by final 200OK with SDP (with audio and video lines and m=application) if flag is enabled then SDP of 200OK should be ignored by the SBC. UPDATE message content: m=application 0 UDP/BFCP (null). 2. Verify the issue. Repeat step 1. UPDATE message content: m=application 0 UDP/BFCP *	The code is modified to ensure the SBC sends m=application line in correct format. **Workaround:** None.

SBX-104851 | SBX-105142	2	PortFix SBX-104851: The SBCb is down and the standby registration with active failed, error 160004. **Impact:** The standby is not allowed to join cluster and fails to start **Root Cause:** The safplus checkpoint file is corrupt and the section needing to be overwritten is not found. **Steps to Replicate:** The root cause of the checkpoint corruption is unknown/cherckpoint corruption cannot be forced and therefore, directly testing this fix is not possible.	The code is modified to re-add the missing section if it is not found. **Workaround:** A complete outage is required as the active must be restarted.
SBX-102469 | SBX-106294	2	PortFix SBX-102469: Time zone is defaulting to EST/EDT on the SBC instances while using image based instantiation. **Impact:** Time zone is defaulting to EST/EDT on the SBC instances while using image based instantiation because the timezone details passed during launch are not being applied when the SBC is brought up. **Root Cause:** The timezone details passed during launch are not being applied when the SBC is brought up. **Steps to Replicate:** Launch the SBC on the SWE. Provide values for timezone and NTP in sbx.conf. Check if proper timezone values and NTP configuration is applied on launch.	The code is modified to update timezone with value in sbx.conf. **Workaround:** No workaround other than setting timezone manually in cli.
SBX-106231 | SBX-107398	3	PortFix SBX-106231: The Metallic noise present in the stream coming out from G722 side. **Impact:** Metallic noise in G722 stream when GPU G722 to Narrow band codec call is made. **Root Cause:** Resampled output is incorrectly copied in GPU G722 Encoder upsampling (narrowband to wideband) code. **Steps to Replicate:** 1. Set sweActiveProfile to use GPU and sweCodecMixProfile to use G722. 2. Make G722 to G711U call. RESULT: G722 stream contains metallic noise.	The code is modified to properly copy the resampled output. **Workaround:** No workaround.
SBX-106343 | SBX-107400	2	PortFix SBX-106343: The GPU EVRCB decoder asserts in Erasure frames simulation test. **Impact:**The GPU EVRCB decoder may crash when there are lost packets in the incoming EVRCB stream, which in turn leads to SWe_UXPAD crash and the SBC application restart. **Root Cause:** Precision errors in the floating point comparison in EVRCB decoder code was identified as the root cause. **Steps to Replicate:** 1. Set sweActiveProfile to use GPU and sweCodecMixProfile to use EVRCB. 2. Make EVRCB to G711U call and do not send the media. RESULT: SWe_UXPAD will crash and the SBC application restarts. **NOTE**: The issue is not always reproducible.	The code is modified to handle precision errors. **Workaround:** No workaround.
SBX-107613 | SBX-107618	2	PortFix SBX-107613: The AMRWB encoder produces corrupted output when channel is reused by lower mode. **Impact:** Degraded audio in AMRWB stream when AMRWB (GPU) call load is running, particularly when each call uses different bitrate. **Root Cause:** Problem occurs when the same codec context is reused and the previous used was for higher bitrate, the root cause was identified due to reinitialization logic for an internal buffer. **Steps to Replicate:** 1. Set sweActiveProfile to use GPU and sweCodecMixProfile to use AMRWB. 2. Make AMRWB to G711U call load using multiple AMRWB clients, each client using different mode. RESULT: Some of the calls may have degraded audio in AMRWB stream.	The code is modified to appropriately reinitialize the internal buffer. **Workaround:** Problem does not occur when all channels use the same bitrate.
SBX-106004 | SBX-106239	2	PortFix SBX-106004: The EMA display error when SMM deleted through the CLI. **Impact:** When a rule is deleted from SMM through CLI and if we try to load the SMM from EMA, an error is displayed in the UI. **Root Cause:** EMA checks the ordering of the rules and if the Order is not continuous then an error is shown in the UI. **Steps to Replicate:** 1. Delete any SMM rule (other than the last) from CLI. 2. Login to EMA. 3. Navigate to **Profiles** > **Signaling** > **SIP Adaptor Profile**. 4. Select the SMM whose rule was deleted from CLI. 5. SMM is shown without any error.	The code is modified to address the issue. **Workaround:** N/A

SBX-105387 | SBX-105936	2	PortFix SBX-105387: LeakSanitizer:SCMP_3 gave memory leaks at MemAlloc2 and same gave Heap overflow issue, both from the same caseID. **Impact:** Heap use after free detected in ASAN for a downstream forking call flow. Accessing memory after it has been freed can cause unexpected behavior and in the worst case potentially coredumps. **Root Cause:** When copying multiple contacts from different downstream forking response, the username of the contact header was not updated from the call block to sip message handle. The Sip Message handle was holding a address that was already freed. **Steps to Replicate:** 1. Run Downstream Forking Call Scenario. 2. UE sends Initial INVITE towards UAS through the SBC. 3. The SBC receives multiple 18x with different to tag and different username in the Contact header. 4. The SBC receives 200 OK for any of the downstream forking dialog.	The code is modified with the correct username from the call block for every downstream forking response. **Workaround:** None.
SBX-106167 | SBX-106808	2	PortFix SBX-106167: The call ends up in one-way audio after the called party puts the call on hold and off hold twice. **Impact:** Call ends up in one-way audio after the called party puts the call on hold and off hold twice **Root Cause:** As a result of call-modify a couple of times, RTCP NAPT learning completes before RTP NAPT learning. This results in RTCP Remote Address being updated, which has remote RTCP Port. Due to incorrect code in RTCP modify flow, remote RTCP port, gets assigned to RTP port. This results in one-way media. **Steps to Replicate:** 1. Run basic SIP to SIP call with NAPT and RTCP enabled. 2. Hold/Unhold the call a few times to check for proper 2-way audio.	Set the correct RTP Port as part of RTCP modify flow. **Workaround:** Since the issue is caused to RTCP NAPT learning completed before RTP during multiple hold/unhold scenario. Work around could be: 1. Disable RTCP or 2. Disable NAPT.
SBX-105804 | SBX-107918	2	PortFix SBX-105804: The CDR field is not populated even though the SBC writes the value to CDR field for '200 Ok of BYE' received/sent. **Impact:** The CDR field added by SMM is not present in the 'STOP' record. **Root Cause:** The SBC was not adding CDR field in the STOP record that was added during the process of 200 response of BYE method. **Steps to Replicate:** 1. Attach the SMM profile which will add the CDR field for 200 response of BYE method. 2. Enable endToEndBye flag. 3. Run a basic A-B call.	The code is modified for updating the CDR field in the STOP record during the processing of response of BYE method. **Workaround:** Add the CDR field in the SMM for BYE method instead of 200 response of BYE method.
SBX-103570 | SBX-106546	2	PortFix SBX-103570: Observed major logs flooding for "MAJOR .SIPSG: sipsgMsgProc.c (-19034) 49487. SipSgRemoveDblTrackingEntry, Hash entry not found" **Impact:** Flood of Error logs are seen during load testing of TLS/TCP Registration and certain Register messages are under the scanner of DBL. **Root Cause:** The DBL has limitations on the offenders list. When this limitation is reached, due to certain bug in the code, the DBL was sending unintended messages to other modules. Due to this message, the flood of logs were observed. **Steps to Replicate:** 1. Execute a 600K TLS/TCP Registration at 1000 rps. 2. Let all the endpoints register. 3. Start the Supported call load (here Approx 20K, 254cps * 90cht= 22860). 50% from the registered Endpoints and 50% from Peering EPs. 4. Ext to Ext IntraSBC Call load of 5000, 50cps*100cht from SIPP. 5. The DBL applied/removed for Registered endpoints should deny entries to 10% of registration /call load. Repeat this for 10 times. 6. Let the load run for 3 hours. 7. Do operator initiated CLI switch-over and revert.	The code is modified to address the issue. **Workaround:** Not Applicable.

SBX-99258 | SBX-108094	2	PortFix SBX-99258: For OOD NOTIFY, SBC sending 481-Call Leg/Transaction Does Not Exist when same SBC acting as P-CSCF and IBCF. **Impact:** SBC fails to send NOTIFY if the User part is not present in the To Header. **Root Cause:** SBC is not able to find the entry in the hash-table as to-tag is not parsed properly, because of user part being absent in the To header. **Steps to Replicate:** 1. Make a basic Subscribe-Notify call, ensure that in From header of subscribe and To header of NOTIFY does not have User part. eg: To: sip:10.xx.x.xx;tag = abcd-1234-012 2. See that for Notify, the SBC will respond with 481 call leg does not exist. 3. Try the same with Fixed build, notify should reach the subscriber. The examples below are To headers that were tested in the Notify: 1. To: sip:10.xx.x.xx;tag = abcd-1234-012 2. To: <sip:10.xx.x.xx>;tag = abcd-1234-012 3. To: sip:xxxx@10.xx.x.xx;tag = aabcd-1234-012 4. To: <sip:xxxx@10.xx.x.xx>;tag = aabcd-1234-012	The code is modified to fetch the tag properly even if the user part is not present in To header. **Workaround:** No Workaround.
SBX-88007 | SBX-106099	2	PortFix SBX-88007: The call flow should work with 5 video and 1 audio streams, which is not working, but when one video stream is removed then the callflow is working. **Impact:** The call fails if peer SDP contains six streams (5 video and 1 audio) and directMedia along with ICE is enabled at the SBC. **Root Cause:** Memory allocated for this SDP was not enough during inter process communication resulted in the failure. **Steps to Replicate:** Configuration: Test requires ingress TG in Zone1, egress TG in Zone2 and AS TG on the SBC, with call to be routed as follows: UE1 -> ingress TG -> AS TG -> AS peer (sipp) -> AS TG - egress TG -> UE2 Enable Direct Media on the ingress and egress TG's (but not on AS TG): TG - media directMediaAllowed enable PSP for all TG's should have DM flag enabled PSP - flags useDirectMedia enable Enable ICE (webrtc) on the ingress and egress TG's: TG - services natTraversal iceSupport iceWebrtc Enable DTLS on the ingress and egress. TG's and PSP's TG - media dtlsProfileName defaultDtlsProfile PSP - dtlsCryptoSuiteProfile DEFAULT enableDtlsSrtp enable Set the directMediaGroupId on ingress and egress TG's to be same e.g. 200 and AS to be different e.g. 400 e.g. TG - media directMediaGroupId 200 Enable Direct Media Anti Trombone on AS TG: TG - media directMediaAntiTrombone enable Steps: 1. From UE1 send an INVITE with ICE and DTLS in the SDP with 5 video and 1 audio stream to ingress TG and route towards the AS TG 2. From the AS send back an INVITE to AS TG of the SBC, the C line of the sent SDP must match the C line of the received SDP. 3. From UE2, send 180 with no SDP followed by 200 OK with ICE and DTLS in the SDP (UE2-sdp 1 audio and 5 video). 4. From the AS send the 180 followed by 200 OK back towards the SBC. Expected Result: The call succeeds. Actual Result: The call fails.	The code is modified so the memory buffer size is increased to accommodate six streams. **Workaround:** None.
SBX-103539 | SBX-105934	2	PortFix SBX-103539: Observed flooded Logs for refresh registration in the Standby SBC restart stop for sometime "sipsgRegSecurity.c (-2745) 1752. SipRaDigestTlsProcessRefreshRegister: No Digest TLS negotiation in progress" **Impact:** The DBG logs were filling up with the following MAJOR level log. 167 09142020 143342.220452:1.01.05.41210.MAJOR .SIPSG: sipsgRegSecurity.c (-2745) 1753. SipRaDigestTlsProcessRefreshRegister: No Digest TLS negotiation in progress **Root Cause:** This is an information message and should not have been getting generated at MAJOR level. **Steps to Replicate:** Run registration call flows.	The code is modified to address the issue. **Workaround:** None.

SBX-106170 | SBX-106189	2	PortFix SBX-106170: The AddressSanitizer: heap-use-after-free on address 0x60f000047d38 at pc 0x562fcd2973a5 bp 0x7f3963983f40 sp 0x7f3963983f38 READ of size 20 at 0x60f000047d38 thread T7. **Impact:** The ASAN reported of accessing a structure pointer that is already freed. **Root Cause:** The SBC is trying to access structure pointer to get socket address, but that structure pointer is already freed in other function. **Steps to Replicate:** Use ASAN build for testing. 1. Send INVITE from UserA, respond from the DNS1 with RCODE error 4 for A query and respond from DNS2 with RCODE 0 with proper DNS answer for A query and check dnsServerStatistics. 2. Run a show command to check the dnsFallback flag and ednsFailures stats: show addressContext <addressContext_Name> dnsGroup <dnsGroup_Name> dnsFallback show table addressContext default dnsGroup <dnsGroup_Name> dnsServerStatistics	The code is modified so now getting socket address from pstSrcAddr structure. **Workaround:** No workaround.
SBX-102115 | SBX-106504	2	PortFix SBX-102115: The SBC modifies the Replaces parameter with wrong Call-ID and tags if the Replaced call was looped back to the SBC through a SIP Proxy that does not modify SIP Call-ID and tags **Impact:** Relay refer with replaces for loopback call, the SBC picks up the wrong call leg. **Root Cause:** The SBC query for the replaces callId, and found matching both legs (loopback). The SBC pick up the wrong leg. **Steps to Replicate:** This is specific to customer call flow.	If loopback is detect, only pick the one with to-tag match local-tag. This is per RFC-3891, section 3. **Workaround:** None.
SBX-106200	2	The DSP is coring and the system unstable **Impact:** Some Fax T.38 IAD calls (T.38 protocols version 3) result in a DSP crash and reload and calls are not successful. **Root Cause:** This condition is caused because this specific V3 IAD is sending CM messages with incrementing UDPTL seq numbers. Typically, repeated messages carry same UDPTL seq number to indicate that they are redundant. Packets with unique seq numbers are assumed to be independent and data from these is causing an unchecked buffer overflow in 3rd party T.38 stack code. **Steps to Replicate:** The main cause of the crash based on core inspection seems to be multiple CM messages with incrementing UDPTL seq numbers Rx by stack. As a result, the test case involves a setting up G711 to V3 call with such CM packets. UAC: start call in G711 and reinvite to V3 and send CM g711v3t38_cmseq.xml UAS: start in g711 and accept a re-invite to silsup-off uas_reinvite_g711.xml PCAP: cmt38seq.pcap Delete beforefix.PKT and afterfix.PKT entries because they refer to files attached to the JIRA, which customers don't have access to. Before fix: The call is set up, and a DSP coredump occurs with a single DSP reload. After fix: The call continues without crash.	The code is modified to address the issue. **Workaround:** Use Version 0 for T.38 calls.
SBX-106429	3	The EMA Configuration Script and Template import page file list doubles each time the search magnifier is used **Impact:** When the search magnifier is hit, the entries are doubled. **Root Cause:** Table with old data is not cleared before starting a new search. As a result, entries were doubled in dataTable. **Steps to Replicate:** 1. Have some entries in the table. 2. Apply a filter and click search button. 3. Entries are not doubled.	The code is modified to clear the data in the table before starting a new search. **Workaround:** No Workaround.

SBX-106583	2	With the Q1912 in a 302 Redirect msg, the SBC sends rn and npdi even though the Contact Header in 302 does not have rn and npdi. **Impact:** When making a call where the INVITE contains NPDI/RN parameters and the SIP variant on the ingress trunk group is set to Q1912 when the call goes through 3xx processing the wrong called party number is sent in the subsequent INVITE. e.g. The initial INVITE contains INVITE sip:11111111;npdi;rn=222222@<IP>:<PORT> The policy dip performs an ENUM query and gets a new called party number of 33333333 The initial INVITE goes out with INVITE sip:33333333@<IP>:<PORT> The end point responds with 3xx and the subsequent INVITE then contains INVITE sip:1111111@<IP>:<PORT> because when using the Q1912 the TOA_PORTED_NUMBER of 11111111 is passed up to in the second policy dip and confuses the routing logic. **Root Cause:** When processing the 3xx and making a second policy dip, the code was meant to remove the generic number parameter of type TOA_PORTED_NUMBER. The code assumed there would only ever be one generic number parameter present. However, when the ingress SIP variant is set to Q1912 the SIP code internally creates a generic number parameter of type additional calling party number based on the contents of the FROM header. In this scenario, the code was unable to delete the generic number of type TOA_PORTED_NUMBER and this was passed back to the PSX in the second policy dip and resulted in routing confusion and unexpected parameter content in the INVITE following the 3xx. **Steps to Replicate:** Perform a call where the SIP variant on the ingress trunk group is set to Q1912 and the INVITE contains the npdi/rn parameters e.g. INVITE sip:1111111;npdi;rn=222222@<IP>:<PORT> The initial INVITE goes out with INVITE sip:3333333@<IP>:<PORT> The end point responds with 3xx and the subsequent INVITE then contains INVITE sip:3333333@<IP>:<PORT>	The code is modified to correctly delete the generic number parameter of type TOA_PORTED_NUMBER associated with the number translation information from the first policy dip to avoid routing confusion on the second policy dip. **Workaround:** If possible change the SIP variant on the ingress trunk group to be "sonus" instead of "Q1912" to avoid the creation of the generic number parameter of type additional calling party number based on the FROM header contents.
SBX-103950	2	There are PAI differences between the SBC and GSX. **Impact:** The SBC was using the ingress calling URI information to create the egress PAI header contents, even when the calling party number digits are all removed using DM/PM rules in PSX. **Root Cause:** Because the SBC supports additional functionality that is not present on the GSX, the SBC can use the contents of the calling URI from the ingress side of the call even when the PSX does not set the username mask flag in the calling URI parameter in the policy response. **Steps to Replicate:** Configure the PSX to generate the PAI header on the egress INVITE, but remove all the calling party digits, all the calling URI username digits and the generic name parameter. Then make a basic call and check that the SBC does not include PAI in the egress INVITE.	The code is modified to check that the PAI header contains username and/or displayname parameters before adding it into the egress INVITE. On the PSX, when the customer wants to delete the calling party number digits, they also need to remove the calling URI username and the generic name information. **Workaround:** Need to use SMM to remove the PAI header.
SBX-106197	2	The PKT port manualSwitch triggered twice. **Impact:** Executing port switchover command from CLI triggers port switchover twice. **Root Cause:** Link detection sub system on standby node subscribes to port switchover action command with CDB (Confd) twice: 1. When the node comes up as standby. 2. When it initiates switchover to become active. When standby node becomes active, executing port switchover command from CLI results in notifying link detection sub system twice due to duplicate subscription. This results in initiating port switchover twice. **Steps to Replicate:** 1. Bring up nodes with port redundancy in HA mode. 2. Initiate CE switchover to make sure standby node becomes active. 3. Execute port switchover command on new active node and validate the behavior.	The code is modified to not subscribe for action command when the node is in standby mode and subscribe only upon switchover when it transitions from standby to active. **Workaround:** None.
SBX-107372	2	Observing lot of errors in DGB files since upgrading to 9.2.0R001. **Impact:** Recently, a fix was added in the SBC for updating the subscription timer on getting a NOTIFY message with the value of expires param in Subscription-State header. But as per RFC 3265 this param is a "should" and is not mandatory. **Root Cause:** When the SBC updated the subscription timer on receiving a NOTIFY message, the case for the expired param missing was not considered. **Steps to Replicate:** Create a subscription on the SBC, with SUBSCRIBE relay. 1. From UAC send SUBSCRIBE to the SBC, which it relays to UAS. 2. Send a NOTIFY without expires param to the SBC from UAS. 3. The log "SipSgStartUpdatedSubscriptionTimer: Invalid subscription timer 0 second for callId" should not be seen after fix.	The code is modified to address the issue. **Workaround:** If it is really required, SMM could also be used to send some expires param in NOTIFY Subscription-State header.

SBX-107999	2	The LeakSanitizer: CpxDnsCreate leaks observed during SBX-85432/<redacted> E2E C-SBC automation run. **Impact:** There is a small memory leak in the Cpx process when DNS elements are added or deleted. **Root Cause:** As part of adding/deleting DNS entries the Cpx process reads in the interface group name from CDB and stores it in a local buffer but does not free it when finished processing. **Steps to Replicate:** Add DNS server entries.	The code is modified to correctly free up the local buffer at the end of the configuration logic. **Workaround:** None.
SBX-107978	2	There are coverity issue in the SIPSG. **Impact:** There are coverity issues for NULL check. **Root Cause:** The null pointer dereferences while handling a session refresh. **Steps to Replicate:** Run a call where re-INVITE does not contain SDP.	The code is modified to add the NULL check before accessing the pointer. **Workaround:** No workaround.
SBX-105105	2	Adjust the MAX_LEN_REALM in camRfAppRedund.h to correct length. **Impact:** If the realm string under realmRoute of a diamNode configuration is configured with more than 129 characters, there is a possibility of the string value not being retrieved correctly from the cdb after the SBC restarts or not being made redundant correctly on a HA system. **Root Cause:** The maximum size for the realm string was incorrectly defined as 129. **Steps to Replicate:** 1. On a HA SBC system, Configure diamNode with a realmRoute that has realm string greater than 129 chars. For example: set addressContext default diamNode DIAMNODE realmRoute RX.EXAMPLE.COM realm ims1111111111222222222233333333334444444445555555556666666666 77777777778888888888999999999000000000011111111122222222233333333333 mnc094.mcc235.3gppnetwork.org peer RX.EXAMPLE.COM appId rx 2. Show addressContext default diamNode to verify configuration has applied correctly and realmRoute has realm value string as configured. 3. Perform a switchover the SBC. 4. On the newly active SBC, show the addressContext default diamNode to verify configuration is the same and realmRoute has realm value string as configured.	The definition of maximum size for the realm string is modified to 257. **Workaround:** The realm string should be limited to 129 characters.
SBX-106687	2	The Platform Interface Status was incomplete. **Impact:** In the Network Tools, the Platform Interface Status section can be used to display the status of Interface selected from the left side section. For certain interfaces like pkt0, pkt1, mgt0, mgt1 the status message was incomplete. **Root Cause:** For interfaces like pkt0, pkt1, mgt0, mgt1 the status message displayed in textarea element, had more than one < and > characters and so the text within them was considered as HTML block by the browser and it was hidden. **Steps to Replicate:** 1. Login to EMA, open **Administration** > **System Administration** > **Network Tools.** 2. Select interfaces in the "Platform Interface Status" section and ensure that the displayed status message matches with the status message from CLI.	The code is modified from <textarea> to <pre> to address the issue. **Workaround:** Not Available.
SBX-104439	2	The SBC is not generating the UPDATE message towards the UAC for the 183 Dialog-2 when there is delay in PRACK message. **Impact:** A call failure was observed during the processing of second dialog provisional response with SDP for downstream forking scenarios when PRACK is delayed at ingress. **Root Cause:** When the SBC needs to send UPDATE at ingress during downstream forking for codec re-negotiation while PRACK is pending, it tries to formulate an internal auto answer. If the UPDATE is offered with a new codec other than previously locked, the SBC while forming such local answer adds the previously negotiated codec. This created a mismatch in offer-answer state machine resulting in call failure. **Steps to Replicate:** 1. Enable customer configurations. 2. Send 183 Dialog-2 from UAS. 3. Once 183 Dialog-2 received to UAC, Send PRACK for that 183 after 2 seconds delay. 4. Check if the SBC sends UPDATE for the second dialog 18x.	The code is modified to consider presence of "doNotAutoAnswer" TrunkGroup flag to decide if a local answer needs to be formed or wait until PRACK comes to release the UPDATE. **Workaround:** Not Applicable.

SBX-104591	2	The SBC is releasing the call during customer-1-1-4 call flow when 200OK answered with dialog-1 and delay in ACK from UAC **Impact:** Call failure observed during processing of second dialog provisional response with SDP for downstream forking scenarios when PRACK is delayed at ingress **Root Cause:** When the SBC need to send UPDATE at ingress during downstream forking for codec re-negotiation while PRACK is pending, it tries to formulate an internal auto answer. If the UPDATE is offered with a new codec other than previously locked, the SBC while forming such local answer adds the previously negotiated codec. This created a mismatch in offer-answer state machine resulting in call failure. **Steps to Replicate:** 1. Enable customer configurations. 2. Send 183 Dialog-2 from UAS. 3. Once 183 Dialog-2 received to UAC, Send PRACK for that 183 after 2 seconds delay. 4. Check if the SBC sends UPDATE for the second dialog 18x.	The code is modified so consider the presence of "doNotAutoAnswer" TrunkGroup flag to decide if such local answer need to be formed or wait until PRACK comes to release the UPDATE. **Workaround:** Not Applicable
SBX-108066	2	The /opt/sonus/sbx/bin/opensslSelftest cmd failed in the SBC 7000. **Impact:** When the FIPS mode is enabled on hwType SBC7000 (7k), services will fail to come up and the SBC becomes inaccessible. **Root Cause:** After enabling the FIPS mode when FIPS selfTests run, opensslSelfTests fails due to using a deprecated SSL engine on SBC 7000. **Steps to Replicate:** 1. Enable FIPS mode from CLI. 2. Ensure the SBC services are accessible after reboot.	The code is modified to remove the deprecated SSL engine from opensslSelfTest and this allows FIPS mode to function as expected. **Workaround:** None.
SBX-107486	2	The EMA display error when the SMM is having criteria with reg-exp like "cpm.msg|cpm.largemsg". **Impact:** The EMA display error when SMM is having criteria with reg-exp like "cpm.msg|cpm.largemsg". **Root Cause:** The EMA is not checking whether nonmatch value is present in database or not. **Steps to Replicate:** 1. Log into the SBC from CLI. 2. Configure the profile rules provided in the Description in the DB. 3. Log into the EMA GUI. 4. Navigate **Profiles**->**Signaling ->sipAdaptorProfile**. 5. Edit the Configured profile that is done from the CLI. 6. There we can see the issue is fixed.	The code is modified to address the issue. **Workaround:** Not Applicable.
SBX-104685	2	The SBC is not triggering UPDATE to ingress and egress for 183 Dialog-2 during E2E precondition interworking. Issue with ISBC(SIP_FW) **Impact:** The SBC was not sending UPDATE towards ingress while process downstream forking call. **Root Cause:** Precondition values are not properly updated in the data structures, resulting in failure to send the UPDATE. **Steps to Replicate:** 1. Bring up customer E2E setup. 2. Transparency precondition scenario. 3. Send 18x dialog-2 with same SDP that of 1st dialog 18x.	The code is modified so now the SBC processes the precondition values and triggers an UPDATE to ingress. **Workaround:** None.
SBX-104624	2	The SBC is not generating UPDATE message for 183 Dialog-2 when 183 Dialog-1 and 183 Dialog-2 having same SDP. **Impact:** The SBC was not sending UPDATE towards ingress while process downstream forking call. **Root Cause:** Precondition values are not properly compared at egress, resulting in failure to send the UPDATE. **Steps to Replicate:** 1. Bring up customer E2E setup. 2. Transparency precondition scenario. 3. Send 18x dialog-2 with same SDP that of 1st dialog 18x.	The code is modified to compare the precondition values and if there is change an indication message is sent to ingress leg which further triggers an UPDATE. **Workaround:** None.

SBX-108029	2	The SIPSG_MSG_PARAM_SIPSG_REDUND_ACT_STR is not registered for serialization correctly before 10.0 release **Impact:** After LSWU, some of the event record fields are not serialized properly for the calls related to Register and OOD messages. **Root Cause:** Event record accounting details are not registered for Serialization. **Steps to Replicate:** 1. The SBC is an older release(< 9.2.1). 2. Configure to generate event record for Register. 3. Make a Register call. 4. Send a Refresh register. 5. LSWU to 9.2.1. 6. Complete the registration call. 7. Check the details of generated event record.	The code is modified to address the issue. **Workaround:** None.
SBX-108025	2	Receiving an unexpected CANCEL in the SBX-SBX GW early media case. **Impact:** 503 is sent for Update because of Server Request not present for Update Request **Root Cause:** Update Server Request is removed from SIP Dialog Structure because we are unable to send a 200 OK for the Update. **Steps to Replicate:** In this scenario Update is received from Egress and it is sent to ingress. In the Ingress, the 200 OK for this Update is delayed and not sent immediately. In the mean time, there is one more Update is received from egress. This is rejected with 500 Internal Error stating request already pending. Now, the 200 OK for the First Update is received from ingress and it is being sent to egress	The code is modified to not remove an Update request from Server request list in the SIP dialog request. **Workaround:** None.
SBX-107243	2	The mid call tracing is collecting only MGSG logs. **Impact:** If the C3 sends MODIFY command with only CallTraceActReq=ON and without any media parameters, then the media logs are not captured in TRC file even if media parameters are changed in subsequent MODIFY command from C3. **Root Cause:** Whenever the MRFP/MGSG receives MOD command with only CallTraceActReq=ON, the MGSG does not send any MODIFY command to NRMA and as a result call tracing info is not updated in NRMA and other media related modules. **Steps to Replicate:** 1. Establish a MRFP call. 2. Send MODIFY command from C3 with only callTraceActReq=ON, no change in media parameters. 3. Send MODIFY command from C3 with changes in media parameters. 4. Verify that .TRC file contains logs from NRMA, XRM and other media related modules.	The code is modified to send modify command to NRMA whenever MGSG receives MOD command with only callTraceActReq=ON. **Workaround:** No Workaround.
SBX-107642	2	The SBC terminates a call as 491 does not get relayed. **Impact:** Run a Scenario with Re-invite without SDP and send 491 request pending for that re-invite. 491 is not being relayed even though relay4xx-6xx is enabled and E2E Re-invite is enabled. **Root Cause:** Even though Re-invite is received from the Network the following bit bIsE2ENtwkReInviteReq in the SIP call structure is not set to true. This is causing 491 to be handled locally. **Steps to Replicate:** Run a Re-invite without SDP scenario and send 491 for that re-Invite.	The code is modified to address the issues. **Workaround:** None.
SBX-104266	2	The SBC is rejecting the call when 200OK of INVITE is answered with Dialog-1 .Dialog-1 is having the AMR-WB codec and Dialog-2 having the EVS codec **Impact:** Call failure observed during certain downstream forking scenarios when 200 OK of initially negotiated dialog comes. **Root Cause:** When the SBC need to send Re-Invite at ingress during downstream forking for codec re-negotiation while ACK is pending, it tries to formulate an internal auto answer. If the INVITE is offered with a new codec other than previously locked, the SBC while forming such local answer adds the previously negotiated codec. This created a mismatch in offer-answer state machine resulting in call failure. **Steps to Replicate:** 1. Enable customer configurations. 2. Send 183 Dialog-1 with the AMR-WB codec. 3. Send 183 Dialog-2 with the EVS codec. 4. 200OK of INVITE sent with the dialog-1.	The code is modified to consider presence of "doNotAutoAnswer" TrunkGroup flag to decide if a local answer needs to be formed or wait until ACK comes to release the Re-Invite. **Workaround:** Not Available.

SBX-93922	2	The SBC is sending Min-Expires header twice to endpoint for 423 Interval Too brief response. **Impact:** The Min-Expires header is sent twice in the REGISTER response. **Root Cause:** The Min-Expires header was sent twice as it was getting added by the application and the transparency profile. **Steps to Replicate:** 1. Enable Min-Expires headers in the Transparency profile. 2. Send a REGISTER message to SBC from UAC. 3. UAS sends 423 response to REGISTER message received from SBC.	The code is modified to address the issue. **Workaround:** Remove the Min-Expires headers from the Transparency profile.
SBX-106995	2	The SBC is not relaying the 183 Dialog-2 towards UAC when it receives UPDATE with preconditions from UAS for Dialog-1. **Impact:** The SBC was not relaying the second dialog 18x to ingress after the completion of preconditions UPDATE for first dialog during downstream forking scenario **Root Cause:** The SBC was consuming the second dialog 18x at egress and skipped further processing. When P-Early-Media value received as part of second dialog 18x had less precedence than that of previous dialog, the SBC did not process the second dialog 18x. **Steps to Replicate:** 1. Bring up the customer E2E setup. 2. From UAS sent 183 Dialog-1 with preconditions. 3. The SBC would send the UPDATE message for the preconditions met for dialog-1 4. UAS sends 183 Dialog-2 with P-E-M sendonly.	The code is modified to follow second dialog 18x and not to consider P-Early-Media value precedence during this process. **Workaround:** Modify the value of P-E-M header to sendrecv using SMM.
SBX-104253	2	The "Deleting the a=maxptime" SMM is not working after an SBC restart. **Impact:** SMM with sdpContent not getting applied after restart. **Root Cause:** At time of restart CPX trying to read SMM with sdpContent from the wrong path. **Steps to Replicate:** 1. Spawned an HA setup. 2. Configured SMM rule with sdpContent and run the scenarios. 3. Switchover the system and re-run the scenario. 4. Switchover again and re-run the scenario.	Fixed the path from where sdpContent will be read for a SMM action. **Workaround:** Delete the SMM rule and configure again.
SBX-105544	2	Dialog scope variable is not present after SMM reject on re-invite message. **Impact:** Dialog scope variable is not present when it is saved in the request which is rejected by SMM reject Operation. **Root Cause:** Dialog scope saved in case of rejected request seems to be not inserted in hash and freed. **Steps to Replicate:** Run a Re-invite call flow and reject the re-invite with 488 and have a SMM Rule to store dialog scope variables for that re-invite,	The code is modified to address the issue. **Workaround:** None.
SBX-108278	2	Enabling the facstate flag can cause healthcheck timeout in SBC. **Impact:** The 'facState' flag if enabled, may result in some potential crash that is caused by health check timeouts. **Root Cause:** The thread that is writing per call key elements in to the file is taking more time and resulting in health check failures. **Steps to Replicate:** Run the calls at 100cps rate for around 5 to 6 hours with flag enabled may hit the health check failure problem.	The code is modified to address the issue. **Workaround:** Disable the facState flag.
SBX-107388	3	Multiple threads are writing to same socket and causing issues. **Impact:** In case of CE_switchover, active went down and standby did not come up as new ACTIVE which led to unstable state until the active becomes stable again. **Root Cause:** To track a healthcheck, the VNFR used a ZMQ mechanism to send/receive messages from VNFCs. As a result, multiple threads tried to write at same time, which caused failure to send messages from VNFR to VNFCs. **Steps to Replicate:** Run multiple CE switchovers with fix.	The code is modified to use the mutex to avoid concurrent writing at same time with its lock/unlock mechanism. If one thread is writing then other threads need to wait in queue until the previous one is not done. **Workaround**: None.

SBX-106850	3	The eventLog combined log size calculation does not consider the disk size properly. **Impact:** For the SBC5400 product, the user is allowed to configure the maximum accounting file size and the maximum number of accounting files so that those files can consume up to 150GB of diskspace. However, the maximum amount of disk space allowed should be 80GB. **Root Cause:** The code that calculates the limit did not properly compute the disk limit if the product was the SBC 5400. **Steps to Replicate:** On an SBC 5400, set oam eventLog typeAdmin acct fileSize 65535 fileCount 2047 [ok][2021-02-17 15:02:03] commit Aborted: 'oam eventLog typeAdmin': The fileSize and fileCount values configured for the event logs would result in a potential combined log file usage of 128.4GB, which exceeds the maximum of 80.0GB allowed [error][2021-02-17 15:02:06] The preceding error message should be displayed indicating that the maximum log file usage is 80GB.	The code is modified to properly compute the limit for the disk limit if the product was the SBC 5400. The disk limit is 80GB. **Workaround**: Ensure that the sum of the filesize*fileCount for each of the SBC log files does not exceed 83886080.
SBX-107162	3	There was an error when dumping System Diagnostics md5 files on the EMA. **Impact:** The checksum files were not shown while generating a system dump through the EMA/PM. **Root Cause:** The EMA/PM only searches for sha256 checksum files now, but the checksum generated was md5, so it was not visible in the list present in EMA GUI. **Steps to Replicate:** Use the EMA/PM to generate System Dump, and verified the presence of sha256 checksum file for every tarball generated.	The code is modified so the System Dump program now generates a sha256 checksum, instead of md5. This is visible to EMA/PM. **Workaround**: None.

Resolved Issues in 09.02.00R002 Release

The following Severity 1 issue is resolved in this release:

Table 32: Severity 1 Resolved Issues

Issue	Sev	Problem Description	Resolution
SBX-106989 | SBX-107017	1	Portfix SBX-106989: Multiple Switchovers occurred because of a DSP core after an Upgrade to V09.02.00R000. **Scenario**: A transcoded call with any Codec<=>G711 and RFC2833 DTMF relay enabled on both legs of a call, and the media probe is disabled. **Impact**: If a peer device sends a RFC2833 without EOP packet (end-of-digit marker), then a DSP crash occurs. **Root Cause**: The code tried to add an error condition (LOST_EOP flag) to media probe data structure without checking whether a media probe was enabled or not. This resulted in a NULL pointer access and a subsequent memory protection fault resulting in a dsp core dump. **Steps to Replicate:** The customer case had a G711A<=>G711A transcoded call with RFC2833 enabled on both legs Use the following setup: SipP UAC=>SBX 5x10 => SipP UAS G729AB(RFC2833) <=> G711(RFC2833) show configuration system media mediaProbe state state disabled; From UAC send dtmf_2833_1_noEop.pcap with '1' digit w/o EOP packets This resulted in dsp core dump before the fix and no core dump was observed after the fix and digit '1' was correctly sent to g711 side.	The code is modified so if the media probe is enabled and not write to media probe structure if media probe is disabled. **Workaround**: Use RFC2833<=>Inband digits or RFC2833<=>SIP Info instead of RFC2833<=>RFC2833.
SBX-103881 | SBX-105740	1	PortFix SBX-103881 to 9.2.x - MEO: Qseries CDR field not matching Qseries format **Impact:** When rn parameter is received as part of SIP R-URI, this value is being used to populate field 10 of the QSBC format CDR record, rather than the received Called Number **Root Cause:** In case of rn parameter received, source for field 10 of QSBC CDR is incorrect **Steps to Replicate:** Send SIP INVITE with R-URI including rn parameter.	Change code such that if rn is received, field 10 of QSBC is populated with the "Called Number Before Translation" (field 24 of Ribbon format CDR). For other scenarios, field 10 is populated as before. **Workaround:** None.

SBX-106206 | SBX-107018	1	Portfix SBX-106206: An existing hairpin call gets silenced after a switchover. **Impact:** When switchover occurs in the SWe SBC Active-Standby HA with the SBC internal loopback media calls flows, the media loopback is not working in existing calls. The looped back media is dropped internally in the SWe NP, because packet skb was not including the internal loopback flag set condition in the NP incoming path validation checks from the internally looped back media for the existing calls. **Root Cause:** When a switchover occurs in the SWe SBC for existing medial calls, a loopback occurs in the SWe NP based on the matching SA. The DA IP address was configured in BRES by setting an internal loopback flag for packet work /skb, even though MAC DA is not updated in BRES flows to the new active instance interface MAC Address to match SA MAC. However, this internal skb loopback flag settings was removed in the release 9.0 release NP refactoring code which caused the packet drops in incoming packet checks for MACs at NP from the looped back media of existing calls. The new calls will not have this issue post-switchover. **Steps to Replicate:** With the SWe SBC Active-Standby HA setup, using AS/3GPP call flow scripts /setup, establish a call that creates the SBC internal loopback media flow. Verify the media flow and then Issue a switchover and verify the media again on this existing active call.	The code is modified to save NP the CPU cycles also while addressing the loopback media issue after a switchover issue for existing calls. **Workaround**: None.
SBX-105269 | SBX-107044	1	Portfix SBX-105269: The SBC crashed and a core dump created. **Impact:** The SCM processes coredump due to NULL pointer access on a pointer that has been freed due to BYE and HOLD REINVITE in a transfer call scenario. **Root Cause:** There was an illegal memory access, absence of NULL check, exposed due to REINVITE. **Steps to Replicate:** A calls B, B REFERs to C and now A and C talk. After sometime, A sends BYE and C sends re-INVITE with a=inactive at the same time.	The code is modified to address the issue. **Workaround**: None.

Resolved Issues in 09.02.00R001 Release

The following Severity 1 issue is resolved in this release:

Table 33: Severity 1 Resolved Issues

Issue	Problem Description	Resolution
SBX-106080	Release 9.2.0 should have CAM version of "00610000". New CDR fields were added in the 9.2.0R0 release, but the CAM version in the top of the ACT header file was not updated to "00610000". It was still set to ""00600000", which was used for release 9.1.0R0. **Impact**: Incorrect CAM version in the top of the ACT header file. **Root Cause**: The code to increment the CAM version was missed. **Steps to Verify Fix:** Run a basic call and check the ACT log header to confirm the CAM version is set to "00610000"	The code is updated to correctly set the CAM version to "00610000".

Resolved Issues in 09.02.00R000 Release

The following Severity 1 issues are resolved in this release:

Table 34: Severity 1 Resolved Issues

Issue	Problem Description	Resolution

SBX-101451	The DSP Threshold setting is not generating a trap on SBC 5400. **Impact:** The g711PacketThreshold, g729Threshold, and g726Threshold onset and abate traps are not sent. **Root Cause:** The NRM did not receive CLI updates to the g711PacketThreshold, g729Threshold, and g726Threshold, and the trap generation code used wrong trap names. **Steps to Replicate:** 1. Provision the threshold levels: set oam traps dspAdmin dspAvailabilityTrap g729Threshold 40 set oam traps dspAdmin dspAvailabilityTrap g726Threshold 60 set oam traps dspAdmin dspAvailabilityTrap g711PacketThreshold 80 commit set oam traps admin sonusSbxDspAvailG729OnSetCrossThresholdNotification state enabled commit set oam traps admin sonusSbxDspAvailG729AbateCrossThresholdNotification state enabled commit set oam traps admin sonusSbxDspAvailG726AbateCrossThresholdNotification state enabled commit set oam traps admin sonusSbxDspAvailG726OnSetCrossThresholdNotification state enabled commit set oam traps admin sonusSbxDspAvailG711OnSetCrossThresholdNotification state enabled commit set oam traps admin sonusSbxDspAvailG711PacketAbateCrossThresholdNotification state enabled commit 2. Configure the trap target: set oam snmp trapTarget EMS160 ipAddress 10.xxx.xx.xxx port 162 trapType v2 state enabled commit. 3. Limit the compression resources to make the issue readily occur: set system mediaProfile tone 98 compression 2 commit. 4. Perform a bunch of transcoded (e.g. G711 to G729) calls that exceed threshold limits, and see onset traps are sent to the trap target. 5. Clear the transcoded calls, and see abate traps are sent to the trap target.	The code is modified to support g711PacketThreshold, g729Threshold, and g726Threshold values. Deprecated the support for allThreshold, as it was never implemented in the SBC. **Workaround**: None.
SBX-102833	Calls are dropping when placed on hold through MS Teams. **Impact:** When MS Teams puts a call on hold and then attempts to retrieve it while the microphone is disabled, the action results in the call being cleared. **Root Cause:** MS Teams performs the call retrieve by sending an INVITE with a replaces message to the SBC and when the microphone is disabled this message includes a=recvonly. The SBC send 200 Ok response to the INVITE with replaces with a=sendrecv while Teams is expecting a=sendonly that causes the call to be cleared by MS Teams. **Steps to Replicate:** 1. Establish a PSTN to Teams call through the SBC. 2. Place call on hold from Teams. 3. Disable the microphone in browser running Teams and then retrieve (place off hold) the call. 4. The call should retrieve should be successful.	The code is modified to respond to an INVITE with replaces containing a=recvonly, with 200 OK containing a=sendonly. **Workaround:** None.
SBX-103974	The STI sends 2 Identity fields in Contact header, but SBC only passes one **Impact:** In the case where multiple "Identity Headers" are present as embedded headers in a 3xx "Contact Header", the SBC sends out only 1 Identity Header for the re-directed INVITE. **Root Cause:** The SBC did not support handling of the scenario where SIP headers are repeated in embedded contact headers in 3xx. The SBC would end up the sending only the last of the repeated headers in the re-directed Invite. **Steps to Replicate:** 1. The SBC is configured with ERE, set the config required for handling embedded headers in 3xx as shown below. "set profiles signaling ipSignalingProfile DEFAULT_SIP egressIpAttributes redirect flags forceRequeryForRedirection enable honorEmbeddedHeadersIn3xx enable" 2. Run a UAS script with 302 redirection and add multiple "Identity headers" as shown below. Ex- Contact: 9710622482<sip:9710622482@10.xx.xx.xx:xxxx?Identity=test1&Identity=test2&Identity=test3> 3. Run a 2nd UAS Script to handle the Redirected INVITE. 4. Run SIPP call, trigger UAC script. Expected Result: The redirect INVITE shall contain both the Identity headers received in 3xx as embedded contact header.	The code is modified to support repeated SIP headers. **Workaround:** None.
SBX-103645	A customer SBC upgrade had a spiltbrain SBC boot issue **Impact:** One of the customer SBCs in N:1 mode is not coming up after upgrade. **Root Cause:** The customer SBC node went for multiple reboots due to config profile change and split brains after upgrade exceeding max limit for reboot. **Steps to Replicate:** Upgrade all customer SBC nodes in one shot so that they all come up together.	The code is modified to avoid split brain due to nodeId/serviceId collision by informing the peer nodes about the self node's nodeId/serviceid as soon as its allocated. **Workaround:** Restart the customer SBC application manually on the node which has exceeded max reboot limit.

SBX-99850	The BYE message was sent to the wrong port. **Impact:** When endpoint is registered over TLS initiates a calls and after call is established, endpoint sends refresh register from modified port and also sends refresh INVITE with no SDP change, the SBC does not send BYE to modified port upon call disconnect. **Root Cause:** The SBC does not update remote connection address when refresh INVITE is received from different port. **Steps to Replicate:** 1. Register endpoint over TLS. 2. Endpoint initiates a call, call gets connected. 3. Endpoint sends refresh register from modified port. 4. Endpoint sends refresh re-INVITE from modified port. 5. Called party disconnects the call. 6. Verify SBC sends BYE to modified port towards caller.	The code is modified to ensure the SBC update remote address when the refresh INVITE is received from modified port. **Workaround:** None.
SBX-86293	PreInstall Check improvements for file permissions. **Impact:** PreUpgrade checks failure due to permission issues on external directory. **Root Cause:** Pre-checks script failed to run commands on peer due to permission issues. **Steps to Replicate:** Perform upgrade to the fix version and verify that upgrade is successful.	The code is modified to ensure permissions/ownership are set properly before running through pre-checks /upgrade. **Workaround:** Set the right ownership for external directory as: `chgrp -R upload /opt/sonus /external/`
SBX-103057	The IAC:terraform apply output is displaying only mgt Active and Standby IP's. I **Impact:** When orchestrating a HFE 2.0 or HFE 2.1 setup in Azure using Ribbon RAF modules, the Terraform output does not show any information about HFE node(s) created, even thought the HFE nodes are started correctly. **Root Cause:** Terraform was missing the configuration to tell it to output the information about the HFE node(s). **Steps to Replicate:** Create a HFE 2.0 or HFE 2.1 setup using Ribbon RAF modules.	The code is modified so that Terraform outputs the management IP and instance name for each HFE node when the orchestration is successful. **Workaround:** None.
SBX-103571	There are call failures due connection toggling between the SBC and SLB. **Impact:** The SBC's can lose connectivity to the HFE nodes when there is high amounts of traffic on the network in Azure **Root Cause:** The health check timeout from the HFE to SBC is too small, therefore was not receiving the replies back from the SBC, causing HFE to switchover **Steps to Replicate:**	Increased the timeout from 20ms to 100ms **Workaround:** Manually edit the following line in HFE_AZ.sh from: $FPING -c 3 -t 20-p 200 ${ACTIVE_SBC_IP_ARR[0]} &> /dev /null to: $FPING -c 3 -t 100 -p 200 ${ACTIVE_SBC_IP_ARR[0]} &> /dev /null
SBX-103058	The IaC is creating same NSG for all the network interfaces created. Recommended SGs should be created for each interface. **Impact:** IaC is creating single NSG for all the 4 sbc interface. **Root Cause:** Iac is creating one NSG and using same for all sbc interfaces created. **Steps to Replicate:** Provided option to create different NSG for different interface created for the SBC. Option available in terraform.vars Ex: sbc_security_group_names = ["TF-SVT-SG-MGT0", "TF-SVT-SG-HA", "TF-SVT-SG-PKT0", "TF-SVT-SG-PKT1"]	The code is modified to create different NSG for different interface of the SBC. **Workaround:** None
SBX-103277	The Active SLB failed in the LCA to coming up "getInterfaceInfoFromMDS: Could not get the interface details in the metadata information!" **Impact:** If the Azure fails on the request when verifying the authorization of the managed identity, then the cloud-init immediately fails. **Root Cause:** The cloud-init is missing tolerance when testing the authorization. **Steps to Replicate:** TBD	Add retries if the connection is reset or times out to address the issue. **Workaround:** Reboot the instance after cloud-init has failed.
SBX-103781	The LeakSanitizer detected memory leaks on various processes for a t140 Call. **Impact:** Small memory leak while configuring SNMP trap targets. **Root Cause:** While processing the configuration requests the SBC code was reading content from CDB into local memory blocks but failed to release the memory blocks at the end of the configuration action. **Steps to Replicate:** Configure the SNMP trap targets.	The code is modified to correctly free the internal memory blocks used to hold the temporary CDB configuration data. **Workaround:** None

SBX-104494	The PES Process cored while testing Flex AD support with the ERE (SBX-72926). **Impact:** PES process dumps core while executing AD service. **Root Cause:** While executing the AD service, PES fetches the AD profile from cache. Since there is no AD profile was configured in this case, cache shall return NULL. The code was missing to check for NULL for the AD profile pointer. **Steps to Replicate:** Configure a AD number translation criteria with ingress TG as the trigger criteria type. Make a call on the ingress TG. While executing the AD service, PES process will core dump.	The code is modified to check for a NULL for AD profile and AD attribute profile. If there is no profiles configured, the control returns and the service is marked as failed. **Workaround:** Configure an AD Profile and AD Attribute profile so that the existing code can be executed further.
SBX-104769	The SCM Process cored while testing SBX H323 Conformance and Interworking. **Impact:** The SCM Process cored while running SIP-H323 interworking call to verify rfc2833 to inband DTMF. **Root Cause:** Accessing of a NULL pointer caused the core dump. **Steps to Replicate:** Run a SIP-H323 interworking call with SIP side RFC 2833 and H.323 side inband DTMF being enabled.	The code is modified to check for NULL pointer before accessing it. **Workaround:** None.
SBX-105263	Observed a PRS Process core followed by a "DsPr, Ssre, Cpx" core on both active and standby box, for the Openstack S-SBC HA pair and "Ccsp" process core on the TSBC active while running calls on the 2CPS with the ASAN build. **Impact:** There was a memory leak detected by the ASAN in the active S-SBC while running the G.711 to G.729 transcoding load on the D-SBC. **Root Cause:** A code analysis of the ASAN reported function revealed that in some corner scenarios, the SBC may end up leaking the memory related to the place holder used to store the remote DSP resource. **Steps to Replicate:** Re-run the same load in ASAN and ensure no memory leaks are detected	The code is modified to free this memory. **Workaround:** None.
SBX-102082	The SCM Process core dump was observed when REGISTER is received and useRandomUserInfoInContactHdr is enabled. **Impact:** Invalid memory access issue when both embeddedRegInfoinUserPart and useRandomUserInfoInContactHdr flag were enabled **Root Cause:** In the SBC, the appropriate memory was not allocated for contactUrl puchUsername in case both embeddedRegInfoinUserPart and useRandomUserInfoInContactHdr flag were enabled, due to this invalid memory access was happening. **Steps to Replicate:** 1. On SLB - Enable remoteDeviceType to access 2. On SBCs enable the embeddedRegInfoinUserPart flag as:- set addressContext <ADDRESS_CONTEXT> zone <ZONE> sipTrunkGroup <TG> signaling embeddedRegInfoinUserPart enabled 3. On SBCs enabled useRandomUserinfoInContactHeader as :- set addressContext <ADDRESS_CONTEXT> zone <ZONE> sipTrunkGroup <TG> signaling useRandomUserInfoInContactHdr enabled	The code is modified to allocate appropriate memory for puchUsername based on embeddedRegInfoinUserPart or useRandomUserInfoInContactHdr enable case. **Workaround:** As per the SBC design, any of the flags below should be enable not both. embeddedRegInfoinUserPart or useRandomUserInfoInContactHdr flag
SBX-98177 | SBX-104816	PortFix SBX-98177: The SBC 7000 TCP window size. **Impact:** Add CLI support to set the kernel parameter net.ipv4.tcp_window_scaling. **Root Cause:** In certain SBC deployment scenarios (a large number of devices running SIP-TLS), the tcp_window_scaling caused small TCP window size. In such cases, the customer had to use Linux command to disable tcp_window_scaling on each SBC node. **Steps to Replicate:** 1. Show initial setting for tcp_window_scaling on both active (SBCSWE01a) and standby (SBCSWE01b) [root@SBCSWE01a ~]# cat /proc/sys/net/ipv4/tcp_window_scaling=1 [root@SBCSWE01b ~]# cat /proc/sys/net/ipv4/tcp_window_scaling=1 2. Use CLI to change the kernel param value and display the changed value on both active and standby. admin@SBCSWE01a% set system admin SBCSWE01 kernelParams tcpWindowScaling disable admin@SBCSWE01a% commit Commit complete. [root@SBCSWE01a ~]# cat /proc/sys/net/ipv4/tcp_window_scaling=0 [root@SBCSWE01b ~]# cat /proc/sys/net/ipv4/tcp_window_scaling=0	The code is modified for setting the kernel parameter net.ipv4.tcp_window_scaling. The Linux command is no longer needed. **Workaround:** Use Linux command to set the kernel parameter on both active and standby. [root@SBCSWE01a ~]# sysctl net.ipv4.tcp_window_scaling=1 [root@SBCSWE01a ~]# sysctl -w net.ipv4.tcp_window_scaling=0 [root@SBCSWE01b ~]# sysctl net.ipv4.tcp_window_scaling=1 [root@SBCSWE01b ~]# sysctl -w net.ipv4.tcp_window_scaling=0 To be persistent across SBC restart and system reboot, use Linux the following shell command on both active and standby. [root@SBCSWE01a ~]# echo "net.ipv4.tcp_window_scaling=0" >> /etc/sysctl.conf [root@SBCSWE01b ~]# echo "net.ipv4.tcp_window_scaling=0" >> /etc/sysctl.conf
SBX-105351 | SBX-105366	Portfix SBX-105351: The 823R0 SCM Process cored. **Impact:**The SCM cores after a long extensive load of the OOD relay. **Root Cause:** The SBC accesses an invalid pointer of link list when the cleanup relay control block. **Steps to Replicate:**System required HW_TYPE_SBS5000 and max support Relay per SCM is 4194304. Run the OOD relay load (Notify). After a long period time (at least 4m relay per SCM).	The code is modified to properly initialize the link list. **Workaround:** None.

SBX-105019 | SBX-105184	Portfix SBX-105019: A crosstalk issue seen on the SBC 5400. **Impact:** When there is a transcoded call with Opus codec and Opus termination does not send any packets to the SBC, then other termination of opus call, may hear audio from another unrelated opus transcoded call or it may hear white noise. This occurs on SBC5x10/5400/7K but not on SWe platforms. This problem only happens if no opus packet is received. When the decoder receives first opus packet, subsequently problem does not happen for that call. **Root Cause:** Initially, when no packet is received, Opus decoder is not called. As a result, the decoder's output buffer is uninitialized and it happened to be stale buffer of another opus call or a leftover buffer of a previous Opus call on that DSP. That buffer is used to encode data for other leg of the Opus call and that results in cross talk audio or distorted noise to other termination of Opus call. **Steps to Replicate:** 1. Make two sipp Opus<=>g711 calls, say call 1 and call 2 on SBC5x10/5400/7K 2. These two calls have to land on same DSP core. So issue a unhide debug command 'request sbx drm debug command "loadbalance disable" before making two calls. Without this command, both calls may not land on same DSP core and you may not see same problem. 3. Call 1 sends audio packet (.pcap) from Opus termination but call 2 does not send any packets to the SBC from it's Opus termination. 4. Call 2's g711 termination will hear audio from call 1's opus termination.	The fix is to clear the buffer (with silence) when the Opus decoder is not primed with any packet. **Workaround:** 1. Use a different codec other than Opus. 2. Use SWe platform instead of h/w SBC5x10/5400/7000.
SBX-102122 | SBX-104540	Portfix SBX-102122: SAM Process core dumps with v06.02.01 F012. **Impact:** The SAM and PRS process cored in the Standby node. **Root Cause:** The DRBD split brain lead to DRBD GI reset. This leads to a DRBD full sync, increasing the i/o congestion and ultimately causing a healthcheck timeout. **Steps to Replicate:** To test, run "drbdadm disconnect mirror". Once we get "standby split-brain" log in DBG logs, run "drbdadm disconnect mirror" again so that DRBD does not connect automatically and we get into the block which we need to test. Run "drbd-overview" and check if drbd does not went for full sync.	The code is modified to perform the DRBD checks after DRBD split-brain recovery. **Workaround:** None.
SBX-102625 | SBX-104065	PortFix SBX-102625: The SIP calls stop in receiving 183 (Precondition). **Impact:** Call stopped working after 183 received without SDP. **Root Cause:** As part of egress precondition interworking, to negotiate the SBC should send an UPDATE to the egress endpoint. When 183 received without SDP, SBC should not try to send UPDATE. SIPSG call state assumed UPDATE is sent. Therefore, when the next 183 is received it tried to queue the 183 assuming UPDATE is in progress. **Steps to Replicate:** As mentioned in the JIRA	The code is modified to avoid this state transition when 183 received without SDP. **Workaround:** Remove the 183 without a SDP message using SMM.
SBX-102837 | SBX-104152	PortFix SBX-102837: The fra-tdg-sonus-01 SipSignalingPorts became OutOfService after a switchover. **Impact:**The SIP sigPorts stuck in the OOS after a switchover. **Root Cause:** The customer had the network/pkt port issue, on one of their HA node, which caused pkt port(s) to bounce randomly, i.e. pkt port went DOWN and came back UP within 2 to 3 seconds. So they have been keeping that node as standby node. They also have link detection enabled for pkt port(s) and have around 100 LIFs per pkt port, one per SIP SIGPORT. When the pkt port went down, NRS delays the port down event processing for 2 second to allow link failure detection to be ready and also to avoid the race condition between NRS and LVM. When a 2 second delay timer is up, the NRS starts to take down affected LIFs and notifies local SIPCM and SIPFE so they can take down affected SIP SIGPORTs. In SIPCM, all the sockets on the affected sigPort are put in a delete pending table and starts a 1 tick timer. Then the socket(s) is being deleted after 1 tick timer is up. When pkt port came back up, NRS processes the event with no delay and notifies SIPCM and SIPFE as well. Since there are around 100 LIFs, there were many messages exchanges between NRS/XRM/SIPCM/SIPFE. NRS LIF FSM has the mechanism in place to handle the timing issue and LIFs were all back in service. But SIPCM failed to activate some SIP SIGPORT(s) while binding the socket(s). These error messages indicated that SIPCM tried to activate the SIGPORT while it was still pending delete. Therefore SIGPORT got stuck in OOS(broken state) in both SIPCM and SIPFE on standby node. If there was a switchover happened later, user would then noticed one or more SIGPORTs were OOS. They have to manually bounce those SIGPORTs to bring them back in service. **Steps to Replicate:** The nature of the problem was the timing caused race condition. There is no good way to re-create/verify the fixes. Suggest to run regular SIP related regression tests.	The code is modified to: 1. Introduce a new 1 tick timer in SIPCM_DATA_STR, activateRetryTimerId. 2. The deletePendingSocketTable and if the sigPort is found in the table, then start the 1 tick timer. When the timer is up, SipCmActivateCallSigPort() is invoked again. Once the sigPort is activated successfully, SIPCM notifies SIPFE as usual. **Workaround:** No workaround.
SBX-101161 | SBX-103677	PortFix SBX-101161: A memory leak was observed in the SAM process. **Impact:** A memory leak was observed in the SAM process. **Root Cause:** There is race condition in the code that handles CALL_AUDITs and CALL_CLEANUPs that can cause a memory leak. If the response to a CALL_AUDIT takes to long, the code that handles the "late" response has allocates memory for a structure that may never get freed. **Steps to Replicate:** This issue is caused by a race condition that cannot be forced - therefore we cannot specify steps to reproduce this issue.	The code is modified to add a timer every time a fault structure is allocated. When the timer expires, if the the structure still exists it will be freed. **Workaround:** There is no workaround.

SBX-104802 | SBX-105186	PortFix SBX-104802: Enabling the Dialog Transparency causes calls to fail. **Impact:** The call fails for the dialog transparency and forking. **Root Cause:** When the ingress support PRACK and multiple 18x fork, the SBC fails to send 200OK to ingress. **Steps to Replicate:** Configure dialog transparency and downstream forking on egress. Ingress support PRACK, egress not support PRACK. The Egress answers 180fork1, 180fork2, 180fork3, and 200OKfork2 simultaneously.	The code is modified so the SBC resets the PRACK pending status properly, causing 200OK stuck in the queue. **Workaround:** Disable the dialog transparency.
SBX-104761 | SBX-105065	PortFix SBX-104761: A SM Process coredump occurred on the server. **Impact:** The SM Process crashed while executing the "show table system syncStatus" command. **Root Cause:** The shell script used to get the oracle sync status - PolicyDBSyncStatus.sh - did not return within 10 seconds, causing a healthcheck timeout that caused the coredump. **Steps to Replicate:** This problem is not reproducible.	The code is modified to disable heathchecks while fetching the syncStatus. **Workaround:** There is no workaround.
SBX-103553 | SBX-105277	PortFix SBX-103553: The SBC does not proceed multiple 183. **Impact:** The GSX-GW-SBX call erroneously queues 183 message at SBX when X-Service-Type precondition is received and downstream forking enabled. **Root Cause:** An interaction between downstream forking and GW-GW code. **Steps to Replicate:** Make GSX -> SBX SIP-GW-SIP call. Egress trunk group has X-Headers supported. Egress trunk group has downstream forking enabled. INVITE --> <-- 183 with X-Service-Type: cf,precondition and SDP <-- 183 with X Service-Type: cf,precondition and different SDP <-- 180 with X Service-Type: cf and SDP <-- 183 with X Service-Type: cf and no SDP This final 183 is queued.	The code is modified to not perform the queueing in GW-GW scenarios. **Workaround:** None.
SBX-104443 | SBX-105071	PortFix SBX-104443: The SM Process and Cpx cores prevented fra-tdg-sonus-01-1 to come back up as standby after switchover **Impact:** The SM Process and Cpx processes cored on slot 1 after LDG triggered switchover to slot 2. The SM Process was deadlocked while retrieving peer NTP status. The Cpx cores happened after SM Process coredump, when writing SMM profiles into shared memory. **Root Cause:** The root cause was SM Process deadlock. **Steps to Replicate:** This is time sensitive issue. The steps cannot be re-produced or verified. Suggest to run full regression test with switchovers.	The code is modified to release smNtpLock_ after issuing a NTP restart command because we certainly do not need the lock while doing the restart. **Workaround:** No workaround.

SBX-103254 | SBX-104839	PortFix SBX-103254: The call setup delay with the Option Ping 40+ endpoints SBC SWe. **Impact:** The configuration support to disable Path MTU Discovery by setting kernel parameter net.ipv4. ip_no_pmtu_disc (ipNoPmtuDisc). When ipNoPmtuDisc is to 2, the DF bit in IP packet header will be set 0. **Root Cause:** The secure network does not support Path MTU Discovery per RFC-1191. **Steps to Replicate:** Testing on a Standalone SBC SWe: 1. Start packet capture, and make SIP call (SIP-TLS). Verify Path MTU Discovery is enabled by checking outgoing IP packet's DF bit is 1. - Test to show the issue [root@SBCSWE03 ~]# date; tshark -t a -i pkt0 -f "ip host 10.x.xx.xx" -w t_tshark_pkt0_10.x.xx.xx_1127_pmtu_1027_01.pcap Tue Oct 27 16:21:11 EDT 2020 Capturing on 'pkt0' 35 ^C [root@SBCSWE03 ~]# tshark -V -r t_tshark_pkt0_10.7.20.29_1127_pmtu_1027_01.pcap | more Internet Protocol Version 4, Src: 10.x.xx.xx (10.x.xx.xx), Dst: 10.xxx.xx.xxx (10.xxx.xx.xxx) Version: 4 Header Length: 20 bytes Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) 0000 00.. = Differentiated Services Codepoint: Default (0x00) .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00) Total Length: 60 Identification: 0x0000 (0) Flags: 0x02 (Don't Fragment) 0... .... = Reserved bit: Not set .1.. .... = Don't fragment: Set ..0. .... = More fragments: Not set Fragment offset: 0 [root@SBCSWE03 ~]# --> The DF bit was set to 1. 2. Disable Path MTU Discovery. admin@SBCSWE03% set system admin sbcswe03 kernelParams ipNoPmtuDisc ? Description: Configure /proc/sys/net/ipv4/ip_no_pmtu_disc (0 (default; disable); 1,2,3 (enabled modes)) 1: when frag-required ICMP is received, PMTU to this destination is set to min_pmut 552. 2: implicitly setting IP_PMTUDISC_DONT on every created socket - outgoing IP packet DF is set to 0. 3: hardened pmtu discover mode. Please refer to Linux kernel document. Possible completions: <int, 0 .. 3>[0] admin@SBCSWE03% set system admin sbcswe03 kernelParams ipNoPmtuDisc 2 admin@SBCSWE03% commit Commit complete. [ok][2020-10-27 16:36:27] 3. Restart the SBC. (If using HA, restart both nodes) [root@SBCSWE03 ~]# date; sbxrestart Tue Oct 27 16:36:56 EDT 2020 4. Start packet capture, and make SIP call (SIP-TLS). Verify Path MTU Discovery is disabled by checking outgoing IP packet's DF bit is 0. [root@SBCSWE03 ~]# date; tshark -t a -i pkt0 -f "ip host 10.x.xx.xx" -w t_tshark_pkt0_10.x.xx.xx_1127_noPmtu_1027_02.pcap Tue Oct 27 16:42:32 EDT 2020 Capturing on 'pkt0' 26 ^C [root@SBCSWE03 ~]# tshark -V -r t_tshark_pkt0_10.x.xx.xx_1127_noPmtu_1027_02.pcap | more ... Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 ... Internet Protocol Version 4, Src: 10.x.xx.xx (10.x.xx.xx), Dst: 10.xxx.xx.xxx (10.xxx.xx.xxx) Version: 4 Header Length: 20 bytes Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) 0000 00.. = Differentiated Services Codepoint: Default (0x00) .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00) Total Length: 60 Identification: 0xe881 (59521) Flags: 0x00 0... .... = Reserved bit: Not set .0.. .... = Don't fragment: Not set ..0. .... = More fragments: Not set Fragment offset: 0 ... [root@SBCSWE03 ~]# --> The DF bit was set to 0, and Path MTU Discovery is disabled.	Disable the Path MTU Discovery by setting kernel parameter net.ipv4. ip_no_pmtu_disc to 2. When set to 2, the DF bit will be set to 0 for the transmitted packets on every created socket. The configuration parameter is "system admin <name of system> kernelParams ipNoPmtuDisc". **Workaround:** The workaround is a hack. It can be used one time test only. The hack will not survive Linux reboots. 1. Make changes on the current Standby (assuming SBC1 is currently active, and SBC2 is currently standby) [root@SBC2 ~]# date; cat /proc/sys/net/ipv4/ip_no_pmtu_disc [root@SBC2 ~]# date; echo “2” > cat /proc/sys/net/ipv4/ip_no_pmtu_disc [root@SBC2 ~]# date; sbxrestart 2. Wait until SBC2 is up and synched. Ensure the p_no_pmtu_disc is set to 2. [root@SBC2 ~]# date; sbxstatus | tail -4 [root@SBC2 ~]# cat /proc/sys/net/ipv4/ip_no_pmtu_disc 2 [root@SBC2 ~]# 3. Make changes on the current Active. [root@SBC1 ~]# date; cat /proc/sys/net/ipv4/ip_no_pmtu_disc [root@SBC1 ~]# date; echo “2” > cat /proc/sys/net/ipv4/ip_no_pmtu_disc [root@SBC1 ~]# date; sbxrestart 4. Wait until the SBC1 is up and synched. Ensure the p_no_pmtu_disc is set to 2. [root@SBC1 ~]# date; sbxstatus | tail -4 [root@SBC1 ~]# cat /proc/sys/net/ipv4/ip_no_pmtu_disc 2 [root@SBC1 ~]# 5. May perform a switchover to make the SBC1 to be active. 6. Run your tests.

SBX-95982 | SBX-104938	PortFix SBX-95982: The SBC was running version 6.2.2 and cannot capture media with MCT. **Impact:** The MCT reload of configuration (sbx restart or switchover) will not succeed. **Root Cause:** Missing small logic during the restart in order to properly reload the MCT configuration. **Steps to Replicate:** Retest MCT reload and switchover scenarios.	The code is modified to properly reload the MCT configuration. **Workaround:** User can delete the MCT config and reconfigure it after any restart/switchover.
SBX-103948 | SBX-103977	PortFix SBX-103948: The SBC Application is crashing when CPaaS to PSTN call is made. **Impact:** The SBC cores after a reboot/upgrade. **Root Cause:** The issue was introduced when the SBC try to support 10000 SMM rules in 8.2.0. **Steps to Replicate:** Configure the customer rules (delete SDP line). Major logs trigger but the rule still success. After a reboot/upgrade, the core occurs.	The code is modified to address the issue. **Workaround:** Disable the delete SDP rule.
SBX-105156 | SBX-105239	PortFix SBX-105156: The SBC was sending m=application 0 UDP/BFCP (null). **Impact:** The SBC generates the syntax error m line UDP/BFCP in 183. **Root Cause:** The SBC accesses the initialize data when format m line for UDP/BFCP **Steps to Replicate:** Incoming call with m-line UDP/BFCP. ERE/PSX using script NO_ROUTE and trigger announcement. The internal 183 has m-line UDP/BFCP with an invalid syntax.	Make the m-line initialize properly to address the issue. **Workaround:** Use the SMM to correct m-line syntax error.
SBX-96239 | SBX-105068	PortFix SBX-96239: The display-name in the Diversion header or History-info header is deleted during the interworking. **Impact:** The SBC does not send display name present in ingress INVITE's diversion header in history info header in egress INVITE. The SBC does not send a display name present in ingress INVITE's history info header in egress INVITE's diversion header. **Root Cause:** The SBC does not consider display name when interworking between diversion header and history info header. **Steps to Replicate:** Ensure the display name is sent in history info header of egress INVITE when the SBC is converting diversion header to history info header. Also, the SBC should send the display name in diversion header of egress INVITE when the SBC is converting history info to diversion header.	The code is modified to ensure the display name is sent when the SBC is interworking history info and diversion header. **Workaround:** None.
SBX-104225 | SBX-105154	PortFix SBX-104225: Both servers are registered but offline, and the SBCs cored after routing the changes from the customer. **Impact:** The S-SBC Core dump with PEM enabled call-flow. **Root Cause:** With PEM enabled, M-SBC performs NAPT learning for 1st RTP Packets. Upon receiving the Napt Indication for egress-leg from the M-SBC, the NRMA on the S-SBC performs flowChange/modification on both ingress and egress leg. As part of this flowChange/modification in ingress-leg, the ingress is NULL, resulting in coredump. The cktInfo on ingress should never be NULL, unless the call is being teared down. In this case, the ingress-leg has received a CANCEL, resulting in the call being taken down, as part of this call tear-down, ingress-leg cktInfo is reset to NULL, and then the de-alloc indication for ingress-leg is sent to the M-SBC, while the S-SBC is waiting for response of this tear-down, it processes the NAPT indication on egress-leg from the M-SBC. This results in the NULL cktInfo pointer getting accesses for ingress-leg. **Steps to Replicate:** 1. Setup a D-SBC transcoded call with MRF. 2. Enable PEM on egress. 3. Ensure PRACK is enabled. 4. Ensure 180 without SDP, followed by 183 with SDP is received from UAS. 5. Ensure CANCEL is received from UAC, while 200 OK from MRF is received, such that the timing of RTP NAPT learning processing and CANCEL processing match. **NOTE**: This is a very tricky issue to recreate, as the timing may vary every time we attempt, it is a matter is few milliseconds.	The code is modified to address the issue. **Workaround:** Disable NAPT or PEM. This workaround will ensure that we do not get to the race condition.

SBX-104561 | SBX-104936	Portfix SBX-104561: The 8.1R5 customer SBC OAMs reaches 90% memory util and then restarts. **Impact:** The memory leak was observed on the OAM node. **Root Cause:** • The XRM and MRM are sending messages through the ICM to NRM. • The NRM is not present/running on OAM. • Since these are non-discardable messages, they will queue forever until we run out of memory. **Steps to Replicate:** 1. Deploy the fix. 2. Monitor memory usage of PRS process. 3. Validate that PRS memory is not increasing.	The code is modified so that these messages are not sent on OAM node. **Workaround**: Before this fix, the workaround is to restart OAM app to recover the memory.
SBX-104484 | SBX-104614	PortFix SBX-104484: The SBC is rejecting the second Update message from the Egress as 500 result into call failure. **Impact:** The SBC rejects 2nd Update from egress due to DLRB feature. **Root Cause:** The first Update SIPS response locally 200OK but not clear the server request message. As result the second Update, trigger the SIPS answer 500. **Steps to Replicate:** Configure the DLRB, Egress response 183 without the SDP, first Update, and the second Update.	The code is modified so after a 200OK response, the SIPS clears the server request so it can handle the subsequent one. **Workaround:** Disable the DLRB.
SBX-104146 | SBX-104303	PortFix SBX-104146: The DNS Process observed a coredump when responding with a RCODE 1 error from the DNS server and deleting a DNS Group in the SBC. **Impact:** The DNS Process dumps core after getting RCODE errors 1,2,4 for a EDNS query and the DNS Group is deleted immediately on the SBC in the monitoring Interval specified in the "ednsRetryAfter" configuration has values ranging from 60 to 180 seconds with 180 being default. **Root Cause:** The EDNS failure timer callback is invoked, upon encountering an EDNS query failure based on the "ednsRetryAfter" configuration. The timer call back function is missing NULL check for the DNS Group **Steps to Replicate:** 1. The SBC configured with EDNS support. 2. The DNS server is configured to respond with the RCODE 1/2/4 error for EDNS query. 3. Make a SIP Call that triggers the EDNS query. 4. Disable the DNS Server and delete the DNS group within 180 seconds.	The code is modified to cancel the EDNS-failure timer, whenever the DNS Group is deleted and the NULL pointer check is added for the timer callback for robustness. **Workaround:** None.
SBX-103207 | SBX-103580	Portfix SBX-103207: The SBC SWe duplicates the audio from call B to call A. **Impact:** If the CN is not negotiated for G711 codec and remote peer still sends CN packets that match default CN payload type (13) then user on other end may hear cross talk audio of completely unrelated channel or hear own reflect audio. **Root Cause:** When a g711 side does not negotiate CN in signaling, the DSP does not initialize Comfort Noise Generation object. However, if remote peer still sends a CN packet that matches the g711 SID payload type configured in PSP (default 13), DSP accepts the packet. It processes that CN packet incorrectly and as a result uses stale voice buffer that happens to be of another channel. This continues until next voice packet for that channel arrives. As a result, we see cross talk audio from the other call during silence period. In some cases, the user may hear own audio also and that is different manifestation of the same problem. This issue is specific to SWe. **Steps to Replicate:** Follow the step described in problem statement of JIRA.	The code is modified to initialize the comfort noise object even though the CN is not negotiated and process CN packets correctly. **Workaround:** Work around 1: Change the default payload type of comfort noise from 13 to something else (say 15) in PSP of peer that is sending CN packets. This will make DSP drop CN packets because payload type will not match. Work around 2: Enable silence suppression on PSP of peer that is sending CN packets and keep CN payload type that matches with CN payload type.
SBX-102704 | SBX-103869	PortFix SBX-102704: Unable to Add or Edit route with # in Destination National, CLI or EMA. **Impact:** User is not able to store few special characters for the destination number field in the route entity. **Root Cause:** The pattern defined for the destination number filed did not allow special characters. **Steps to Replicate:** Create a route with special character like #123 for the destination number filed in the route entity.	The code is modified to allow only few specific special characters. So, reverted back the pattern to same as before 8.1 release, so that no customers face similar issue again who have configured special characters prior to 8.1. **Workaround:** None.
SBX-102290 | SBX-104913	PortFix SBX-102290: The DBG file was filling up with messages "SIPCM: *ThreadPool: messageSequence". **Impact:** The DBG logs can be overrun with "SIPCM: *ThreadPool: messageSequence" messages. **Root Cause:** The DBG logs can be overrun with "SIPCM: *ThreadPool: messageSequence" messages, when Double CRLF "pings" are received by the SBC over UDP transport. **Steps to Replicate:** Send Double CRLF "pings" over UDP to the SBC.	The code is modified to properly dispose of Double CRLF "pings" received by the SBC over UDP. **Workaround:** Inhibit the transmission (or reception) of Double CRLF "pings" over UDP.

SBX-104934 | SBX-105024	PortFix SBX-104934: The SBC generates the same ICID for more than 1 call, porting the fix for SBX-101887 into 8.2.3F1 did not help **Impact:** Duplicate the ICID generated for two different calls. **Root Cause:** The instance specific value is set to 0 every other call causing the ICID generation to always use 0 in all instances. This results in the same ICID generated in more than one SCM instance when the calls land within the same microsecond **Steps to Replicate:** Configure the SBC to generate ICID on the egress side. Run call load and check for duplicate ICIDs.	The code is modified to manipulate the last octet of the MAC address used in ICID generation. **Workaround:** None.
SBX-105417 | SBX-105583	Portfix SBX-105417: During an S-SBC and M-SBC cyclic switchover, the S-SBC app did not come up after few switchovers. **Impact:** The service did not come up after a switchover due to inconsistent encryptedStore. **Root Cause:** The store became inconsistent after the oam_config got applied, the time taken during deletePeerEntries should also be reduced to allow a ChmClearEncryptedStoreOfPeers to finish faster during startup. **Steps to Replicate:** Perform multiple switchovers and ensure that: 1. ChmClearEncryptedStoreOfPeers does not take too long during startup. 2. The deletePeerEntries runs in background and does not take too long either. 3. The service comes up, role is assigned successfully and store is consistent.	The code is modified so: 1. deletePeerEntries run in background 2. decryptStore validates if decryption was successful to ensure the store is not inconsistent/corrupt. **Workaround**: None.
SBX-103629 | SBX-103654	PortFix SBX-103629: The SIP registrations are failing, and the SBC reporting REGISTER_PARSE_ERROR and replies with SIP 500 when it receives retransmitted initial REGISTER (CSEQ 1) followed by REGISTER with Authorization header (CSEQ 1). **Impact:** When the SBC recv rexmit of registration (cseq=1) after sending 401/407, the SBC relay to AS. At the same time, the IAD sends new registration(cseq=2) for authentication. It triggers race condition to the SBC and response 500. **Root Cause:** The SBC should relay rexmit (cseq=1) registration to application server. **Steps to Replicate:** The IAD send registration(cseq1) to AS, AS response 401 to IAD, IAD rexmit the same sceq1, and send a new sceq2 with auth header.	The code is modified to response rexmit request (cseq=1). So that a subsequent one cseq=2 can handle properly relay to AS. **Workaround:** None.
SBX-105486	The SBC 9.1 MD5 check sum. **Impact:** The SBC qcow2 image is shipped along with a sha256 checksum but Openstack glance supports only md5 checksum. Unable to validate the image in an automated way. **Root Cause:** Checksum was updated from md5 to sha256 as md5 is weaker compared to sha256 algorithm and there are reported attacks on md5. **Steps to Replicate:** With the fix build, ensure qcow2.md5 is one of the build artifacts.	The code is modified to facilitate openstack glance image verification. **Workaround:** User can manually create md5 checksum by running below command: md5sum sbc.qcow2 > sbc.qcow2.md5
SBX-104284	The SNMPv3 traps from the MRFP are not displayed in EMS Fault Management. **Impact:** The traps were not getting displayed in EMS. **Root Cause:** The SBC generates Engine ID at the time of ISO installation. Due to this, all cloud instances share same engine id from the qcow2 generation time. When same engine id is returned by two SBCs in different cluster, the EMS is unable to differentiate between them. **Steps to Replicate:** Launch instances from qcow2 in different clusters. Traps generated should be shown correctly now.	Engine ID is created at the time cloud instance launch now to address the issue. **Workaround:** None.
SBX-104688	Configure the import issue. **Impact:** The fields that supports \r like regex fields, changes it after a configuration Import(XML based). **Root Cause:** The \r is not xml encoded when parsing intermediate xml file. **Steps to Replicate:** 1. Create SMM Profile with regex that has \r export configuration as xml-tar clear DB. 2. Import the configuration. 3. Verify SMM profile regex field.	The code is modified to handle \r as a special case. **Workaround:** None.

SBX-104463	Observed a SCM Process coredump in the gcored while running the 30 SWOs on 7000 Platform. **Impact:** In case of switchover and switchback while running load, we expect some stale entries in SIPSG and CC control blocks. Such entries are cleared on the audit, but while clearing the SIPSG is sending accounting message to CC. This SIPSG was reconstructed, but in CC the index corresponding to this GCID was allocated to some other GCID. When the CC receives such message, the mismatch occurs and it logs a crash in sensitive mode. **Root Cause:** During load run with multiple switchovers, various call modules get reconstructed when standby transitions to active. Due to this some stale entries are expected. If one of these stale entries sends some message (e.g accounting message) and if index for that call was allocated to another call, this error can happen. In case of such mismatch the SBC logs a crash in sensitive mode. **Steps to Replicate:** Load run with multiple switchovers.	If the GCID sent from SIPSG module in accounting message is different from the GCID received in CC module, for switchover case do not do a sensitive crash. Instead add a major log to address the issue. **Workaround:** Run load scenarios in normal mode instead of sensitive mode.
SBX-104526	The emssftp fails in the 9.1R1. **Impact:** The emssftp login was failing. **Root Cause:** The sequence of asking for a password and keep credentials in sync caused the emssftp password failed. **Steps to Replicate:** Checking login, after multiple reboots, rebuild with 1:1 and N: 1, along with 1-2 EMS registered.	The code is modified on the mode(HA vs standalone), included a new script to handle password request and updated for some HA cases. **Workaround:** None.

The following Severity 2 and 3 issues are resolved in this release:

Table 35: Severity 2-3 Resolved Issues

Issue	Sev	Problem Description	Resolution
SBX-104962 | SBX-104989	2	Portfix SBX-104962: The HFE setInterfaceMap() can be incorrect. **Impact:** The HFE_AZ.sh script can configure the HFE node incorrectly if the IP of an interface is a contained with in another. **Root Cause:** The logic used to determine which interface associates while the NIC can find the incorrect interface. **Steps to Replicate:** Create a HFE where the eth0 address contains either eth1 or eth2 IP address.	The code is modified to verify it the only the correct IP address is used. **Workaround:** Request an updated HFE_AZ.sh script from Ribbon. Replace the HFE_AZ.sh in the storage account and reboot the HFE node (s).
SBX-104156 | SBX-104571	2	Portfix SBX-104156: The RTT-TTY support verifies the call flow in the SBC. **Impact:** Lower case characters from t140 packet were not getting converted correctly to Baudot (tty). Also, some other characters were not getting converted as per V.18 A2 table. **Root Cause:** The translation table from T140 to Baudot(TTY) only accounted for the subset of characters that were present in the Baudot (TTY) character set. **Steps to Replicate:** 1. Setup a T140=>Baudot (AMRNB=>G711) call. 2. Create t140 pcap file with all UTF8 characters (128) and validate the baudot generation. 3. Create a t140 pcap file with multi-byte sequence and validate the baudot.	The code is modified to: • The t140=>Baudot translation table as per V.18 Annx2. • Validate multi-byte (2,3 and 4 bytes). • Handle the Byte Order Mark (BOM). • Ignore an invalid byte sequence and substitute the valid but unknown multi-byte seq with an apostrophe. **Workaround:** None. Instead of lower case letters use upper case letters.
SBX-96783 | SBX-104926	2	PortFix SBX-96783: Some counts in the callCurrentStatistics keep incrementing. **Impact:** The "activeRegs" counter provided by the CLI zone callCurrentStatistics/ callIntervalStatistics command may continuously increase. **Root Cause:** Badly formed SIP REGISTER messages received by the SBC (i.e., a REGISTER message that the SIP parser determines is bad) will increment the "activeRegs" counter and never decrement it. **Steps to Replicate:** Send bad SIP REGISTER message(s) to the SBC, and see that the "activeRegs" counter provided by the CLI zone callCurrentStatistics / callIntervalStatistics command increases (and does not decrease).	Decrement the "activeRegs" counter when the SIP REGISTER message fails the SIP parser to address the issue. **Workaround:** None.

SBX-102364 | SBX-104657	2	Portfix SBX-102364: The SBC behavior is inconsistent with the isfocus parameter handling. **Impact:** Issue 1: The SBC is not transparently passing the complete Contact header in 200 OK of SUBSCRIBE when there is a isfocus parameter. Issue 2: The SBC is not adding the Record-Route in any message when doing a full Contact header transparency **Root Cause:** Issue 1: The SBC passes contact header transparently only when the isfocus is present in request as well as response and would not send the contact header transparently only when the contact header in response has isfocus parameter. Issue 2: The code to add a record route for notify and its response is not present. **Steps to Replicate:** 1. Configure the SBC for A to B call. 2. Enable the flag contactTransparencyForIsFocusMediaTag on both TGs. 3. Make a SUBSCRIBE-NOTIFY call flow.	Issue 1: The code is modified to check if the service bit is not set (for the response) and check if the contact header has the isfocus parameter, if the parameter is present, set: SIP_SERVICE_TYPE_CONTACT_TRANSPARENCY_ FOR_ISFOCUS_PARAM for a single contact scenario. Issue 2: The code is modified to add the record route for notify and its response if isfocus parameter is present. **Workaround**: None
SBX-103988 | SBX-104547	2	Portfix SBX-103988: The ICE not working after upgrade to V08.02.03A950. **Impact:** When a call with ICE changes from direct media to passthrough, ICE learning does not get enabled on the call. **Root Cause:** The code was not re-enabling the ICE FSM to start ICE learning when changing from direct media to passthrough. **Steps to Replicate:** Test 1 -------- 1. Establish a call with ICE on ingress and xdmi on egress. 2. Send re-invite from egress without xdmi and complete the re-invite related signaling. 3. Send stuns to ingress media to complete ICE learning and verify call state changes to established and media can be exchanged between ingress and egress.	The code is modified to re-enable the ICE FSM when changing from direct media to passthrough to allow the receipt and processing of stun messages to complete ICE learning. **Workaround**: None.
SBX-103496 | SBX-103806	2	The MGT0 cannot reach the GW. **Impact:** The mgt0 interface appears to be inactive. The user cannot ping the gateway from the SBC 5400. The ethtool -S mgt0 shows the tx_pause count rising rapidly. **Root Cause:** This problem is specific to the SBX 5400 fix. The SBC 5400 has a backpressure mechanism for management ports so that when the receive buffer exceeds a certain level, Design sends pause packets out to the interface to ask the switch/router to pause transmission momentarily. The receive buffer count is incremented by a hardware module and decremented by software. The notification was sent from Network Processor to application about sRTP Rollover Counter (ROC) reset is specifying the wrong interface so software decrements the wrong receive buffer count. This causes the receive buffer count to wrap around, resulting in a high value. This triggers the back-pressure mechanism and Design continuously send out pause packets. **Steps to Replicate:** 1. Set up a pass-thru SRTP call. 2. The call should be a long duration call so that the Rollover Counter (ROC) in the sRTP packet becomes non-zero. 3. Modify the call so that the sRTP packet's the SSRC changes. **Update**: 1. Do a long duration sRTP call (about 30 minutes.) 2. Hold the call. 3. Unhold the call. 4. As a result, this causes an SSRC change and triggers the problem.	Set the correct interface information in the notification to address the issue. **Workaround**: Please contact Ribbon support for a script that will restore contact to the management interface.

SBX-103922 | SBX-104649	2	Portfix SBX-103922: There was a PRS Process coredump on an active/A node in the middle of an upgrade. **Impact:** The PRS Process cored during the LSWU while syncing ICE call data. **Root Cause:** The ICE redundancy code is taking a long time to sync the call data with the standby during LSWU, causing a Healthcheck timeout and a core dump. **Steps to Replicate:** The issue cannot be reproduced easily.	The code is modified so the ICE syncs the call data to standby and addresses the issue. **Workaround**: None.
SBX-104704 | SBX-104907	2	PortFix SBX-104704: Duplicate the audio entries in the route PSP. **Impact:** The duplicate codec entry is being sent in the policy response. **Root Cause:** The function popPSPCodecEntryHlp that populates the codec entry was called twice, and as a result the codec entry was getting populated twice in the TLV. **Steps to Replicate:** Add more then 4 codec entries in the ingress PSP and egress PSP. This will cause the issue to be reproduced.	The code is modified so that the duplicate codec entry is not passed on the d+ response. **Workaround:** None.
SBX-101575 | SBX-104914	2	PortFix SBX-101575: There was an offline upgrade failure from 8.2.1 to 8.2.2 **Impact:** An offline upgrade on a HA setup failed for the upgrade from 8.2.1 to 8.2.2. **Root Cause:** An offline upgrade failed due to presence of a model update marker files that should not get created in case of offline upgrades. **Steps to Replicate:** Perform an offline upgrade on a HA setup to the fix build and ensure upgrade is successful.	The code is modified to ensure nodeB is powered-off/shutdown (instead of the sbxstop) while upgrading a nodeA. This ensures that the model update related markers files do not get created. **Workaround:** None.
SBX-104668 | SBX-105128	2	PortFix SBX-104668: The SNMP PM collection is not working for newly added KPIs. **Impact:** SNMP stats collection at EMS for G711_WITHOUT_XCODE_RES_PEAK_COUNT and G711_WITHOUT_XCODE_RES_AVG_COUNT of DspResDspUsageIntervalStats failed. **Root Cause:** Some of the KPI stats fields are made obsolete as they are no longer supported. Due to this change EMS is not able to collect the stats through SNMP. **Steps to Replicate:** Verify EMS SNMP walk should not fail when queried to the SBC. 1. Bring up SBC. 2. Register SBC to EMS. 3. Enable the sonusDspResDspUsageIntervalStatistics. Expected Result: The EMS fetches stats from the SBC.	The code is modified so the EMS is able to collect stats using SNMP. **Workaround:** None.
SBX-103175 | SBX-103652	2	PortFix SBX-103175: The large microflow profile was not getting enabled in the Custom Traffic Profile. **Impact:** There are multiple issues: 1. For a default profile, max subs was always set to 256K. 2. For the custom and standard traffic profiles, the micro flow count in the NP resource was not proper. 3. Limited support of the 2M micro flows for standard profiles. **Root Cause:** 1. The large micro flow support was not there for the custom traffic profiles. 2. For standard and default traffic profiles, there was restricted /incomplete support of large micro flow that is made generic as part of this issue. **Steps to Replicate:** 1. Create an instance with 10GB memory and 16vpcu with the default traffic profile.Check microflow limits using "/opt/sonus/bin/cpsi -d summary" command. 2. Increase the memory to 50GB memory and check the microflow limits using "/opt/sonus/bin/cpsi -d summary" command. 3. Create a instance with 20GB memory and 16vpcu. Create and activate a custom traffic profile with access enabled in call mix. Check microflow limits using "/opt/sonus/bin/cpsi -d summary" command.	The code is modified to: 1. Introduce a new estimation parameter maxSubs based on the micro flow count is decided and the NP hugepages are reserved. 2. Enable the large micro flow support for all the standard/default profiles where mem > 48GB and vcpu_count >10. **Workaround:** No workaround available. Need to use the build after the fix.

SBX-104347 | SBX-104735	2	PortFix SBX-104347: The resource mem congestion level 3 is approaching threshold 90 sample 82. **Impact:** The SIPCM is leaking a structure that is associated with the SIPMM functionality. **Root Cause:** The code to free this memory under certain error/edge scenarios is missing. **Steps to Replicate:** Since the exact call flow is not know that caused the customer to hit the error condition, no test steps can be used.	The code is modified to free the SIPMM related structure in error scenarios. **Workaround:** Since the exact call flow is not know that caused the customer to hit the error condition, we cannot suggest a workaround.
SBX-102707 | SBX-104911	2	PortFix SBX-102707: The network interfaces are not renamed as expected after an upgrade from 820R2 to 821R0. **Impact:** Network interfaces are not properly mapped when the system is abruptly brought down after the first boot and rebooted. **Root Cause:** Cloud-init service runs in parallel to sonusudev service and can cause issues with the network interface mapping as it tries to rename the interfaces. **Steps to Replicate:** Reboot the system after sonusudev is run on first bootup.	The code is modified to start only after the sonusudev has run and mapped the interfaces properly. **Workaround:** Reboot the instance again to recover from the issue.
SBX-99208 | SBX-102666	2	PortFix SBX-99208: The SBC has the same issue as SBX-86420, this time for an outgoing REGISTER messages. **Impact:** When the TLS port is not sent from the PSX, the SBC is not sending the DNS SRV query to the DNS server. **Root Cause:** The root cause was the SBC just increments the port number by 1 sent by the PSX even if peer port was Zero. **Steps to Replicate:** 1. Configure the SBC and PSX to send a register and subscribe SIP request to relay. 2. Configure the serve FQDN and zero for the FQDN port. 3. Send a register/subscribe request. 4. The SBC should send SRV query to the DNS server.	If port number sent by PSX is zero then do not increment it by +1 by default for selecting TLS port to address the issue. **Workaround:** None.
SBX-103561 | SBX-103793	2	PortFix SBX-103561: The "tgrp" parameter are not passing transparently when the SIP in the core is enabled. **Impact:** The SipCore calls is passing the wrong TGRP parameter value. **Root Cause:** There was missing logic to support the SipCore. **Steps to Replicate:** Configure the SipCore feature. Both the IPSP core and egress leg have "originating Trunk Group Options" set to "Include Tgrp with IP address" Make a SipCore call.	The code is modified to support the SipCore feature. **Workaround:** None.
SBX-103852 | SBX-103978	2	PortFix SBX-103852: The SBC sent an unnecessary 481 for PRACK when the CANCEL is received. **Impact:** The SBC sends unnecessary 481 for PRACK when received CANCEL. **Root Cause:** The issue was introduced by intercept feature (SIP_EVENT_PRACK_INTERCEPT_RCVD). When the SBC received PRACK, it save the message into the server list. Later the CANCEL arrives, UasCancelRequestCmd, the UAS found the message in server list, and thought PRACK is not completed therefore it try to send 481. **Steps to Replicate:** A calls B, B response 180 and send 180 to A with PRACK required. After 32 seconds A sends a CANCEL, the SBC sends an unnecessary 481 PRACK.	Once the 200OK for PRACK has send out, the SIPS deletes the PRACK message in the server list to address the issue. **Workaround:** Enable the e2e PRACK if the egress also supports PRACK.
SBX-96788 | SBX-103979	2	PortFix SBX-96788: The DTMF 2833 PT change (in offer) has incorrect OA SBX handling (wrong answer PT). **Impact:** When the peer offer with new PT, the SBC is unable to process and respond to the previous one. **Root Cause:** There was a logical error that checking the wrong field to detect PT change. **Steps to Replicate:** A call B and connect with "0 100". An INVITE with an offer new PT "0 101". The SBC responds with "0 100".	The code is modified to check the correct field for PT change. **Workaround:** None.

SBX-105428 | SBX-105440	2	PortFix SBX-105428: Error when attempting to delete negative cache record upon a probe response. **Impact:** The DNS query was not out sent from the SBC if a call is made immediately after the DNS server is recovered from a blacklist. **Root Cause:** Due to record is in the negative cache entry from earlier DNS dummy query, the SBC was not sending a query. **Steps to Replicate:** 1. Configure the SBC with a basic call and also configure the DNS group. 2. Ensure that DNS server does not respond to the DNS query or stop DNS server. 3. Now make call and SBC query for DNS server for resolving FQDN, but DNS server is down and there no response from DNS server. 4. After retransmission's timeout value. DNS server will be blacklisted. 5. Now the SBC keep probing DNS server. 6. Bring the DNS server up. 7. The SBC receives probe response, DNS server is removed from Blacklist. 8. Immediately make SIP call. Expected Result: • The SBC selects a DNS query.	As soon as the DNS server is removed from blacklist entry, those records involved with the DNS Dummy query is removed from the negative cache and resolves the issue. **Workaround:** None.
SBX-105010 | SBX-105155	2	PortFix SBX-105010: Observed a congestion for the G711 to G711 transcode calls even before the CPU resource limit is exhausted. **Impact:** The G711-G711 transcoded capacity test shows a lower capacity. (Test is Pump make and break g711 to g711 transcode calls on one of the active instances with 50cps, 90 CHT and 4500 calls). **Root Cause:** The root cause is an incorrectly built libfmtd.a that was built with a debug option and makes the FMTD module take more cycles. This bug was addressed originally in SBX-104122. **Steps to Replicate:** Perform a test indicated in SBX-105010.	The code is modified to remove the -g flag and using -O3 flag for compilation (Port of SBX-104122). **Workaround:** None.
SBX-105072 | SBX-105150	2	PortFix SBX-105072: Password padding with random characters by the SBC causes the RADIUS server to reject the password. **Impact:** The radius password sent to the server has no zero characters at the end following the password and a NULL. **Root Cause:** The radius passwords are padded to 16 characters. The existing implementation did not set those padded characters to 0. **Steps to Replicate:** 1. Configure a radius authentication server. 2. Use a password that is less than 15 characters long for the external radius user. 3. Set the externalAuthententication to true. 4. Run a tshark session. 5. Login to the CLI. 6. Stop the tshark. 7. View the radius password element in wireshark after configuring the shared secret in wireshark under protocol preferences.	The padded characters are now set to 0 to address the issue. **Workaround:** Use 15 or 16 character passwords.

SBX-66831 | SBX-103723	2	PortFix SBX-66831: Need to update/add proper warning message when deleting the ipInterface. **Impact:** The warning message does not display in the cloud SBC when deleting the IP interface, but there is no problem with functionality. **Root Cause:** This is working fine in the hardware SBC. We have the problem in the cloud SBC because when displaying the warning message, we checked few values if that values are matching. Then, show the warning popup but in case the cloud SBC values index are different and check is failing because of that, we are unable to show the warning popup when we delete IP Interface. **Steps to Replicate:** 1. Login to EMA. 2. Go to **All** -> **Address Context** ->**IP Interface Group** -> **IP Interface**. 3. Click on **New IP Interface** button. 4. Fill the correct info in text field, select state as enable, Mode as In Service and click on save button. 5. The creation should be successful. 6. Select the same entry from IP interface list section and click on **delete** button. 7. We should be able to see warning popup like "'addressContext PPP_AC ipInterfaceGroup PPP_IG ipInterface': Deleting ipInterface while in dryUp action can cause problems with calls on the ipInterface. Use force action to clear existing calls on the ipInterface before deleting. Do you wish to continue?"	The code is modified to handle the Cloud SBC scenario. **Workaround:** None.
SBX-100286 | SBX-103102	2	PortFix SBX-100286 to 9.2: The trace file containing SIP Rec PDU was not imported in Ribbon Protect properly. **Impact:** When a level 4 call trace is active, if a SIP PDU is too large to fit on a single trace line, it is split over multiple lines. However, the Ribbon Protect only reads the first line - there is no way for it to know subsequent lines are continuation lines. **Root Cause:** Design issue. **Steps to Replicate:** 1. Enable level 4 call trace. 2. Send a SIP PDU to be traced towards the SBC of total size 2000 bytes.	The code is modified to put the same header onto each level 4 trace line. Include in the header two new fields, the MSG ID and PART to allow Ribbon Protect to recombine multiple trace lines to recover the original message. The equivalent Jira VIGIL-17137 is required for Ribbon Protect compatibility. **Workaround:** None.
SBX-100590 | SBX-104867	2	PortFix SBX-100590: The wrong "Egress Zone Name" in ATTEMPT CDR for a GW-GW call. **Impact:** For a call with multiple routes that include one or more local routes followed by routes on another gateway (for GW-GW) scenario, if the local routes fail and then other gateway route is selected, the resulting ingress gateway CDR for the call has incorrect egress zone name and ID. **Root Cause:** When there are multiple routes, when a route fails the call cranks back to use the next route. When selecting the next route the code is not clearing the internal CDR information for the egress zone. So if the next route selected is on another gateway, the CDR information retains the egress zone information from the previous attempt rather than being blank. **Steps to Replicate:** 1. With the SBC GW-GW setup create two routes for a call such that: - route 1 is routed through local egress trunk group on SBC1. - route 2 is routed through egress trunk group on SBC2. - Set crankback profile to enable attemptRecordGeneration and add reason 41 (503 is mapped to 41 in default SIP to CPC mapping profile). 2. Send a valid INVITE to the SBC1 ingress that will first select route1 and route out through the egress trunk group on the SBC1. From the egress endpoint reject that call attempt with a 503 Service Unavailable. 3. The call will crank back and re-route using route2 through the SBC2 egress trunk group. From the egress endpoint reject that call attempt with a 503 Service Unavailable. 4. Check there are two Attempt CDR records for the call on SBC1. a. ATTEMPT1 - should have the "Egress Zone Name" and "Egress Zone ID" fields populated correctly with zone information for zone of SBC1 egress. b. ATTEMPT2 - should have the "Egress Zone Name" empty and "Egress Zone ID" as 0 because this is an attempt for GW-GW route.	The code is modified to clear the internal CDR information for the egress zone when one route fails and the next route is selected. **Workaround:** None.

SBX-74991 | SBX-104980	2	PortFix SBX-74991: Saving changes to a SMM profile after doing an edit /update operation is taking long time[8 to 16 minutes]. **Impact:** The SIP Adaptor Profile with 250+ rules takes lot of time to create a profile including the update as well. **Root Cause:** When the SIP Adapter Profile with more than one rule is created, each rule is committed individually. However, after each commit EMA internally retrieves all the SIP Adapter Profiles along with their rules, though this is not required it is causing slowness of both create and update operation. **Steps to Replicate:** 1. Login to EMA. 2. Navigate to Sip Adapter Profile Screen. 3. Create a profile with 200+ Rules. 4. Click on Save button.	The code is modified to prevent retrieval of sip adapter profiles after each commit **Workaround:** The only workaround is to create the profile from the CLI.
SBX-101769 | SBX-104912	2	PortFix SBX-101769: The SBC sends the wrong SDP in 200 OK for UPDATE received from the Ingress during tone play(LRBT). **Impact:** The SBC responds with wrong codec in the answer to UPDATE received on ingress/calling side while local ring back tone is playing. As a result, the UPDATE is being used to change the codec on ingress. In this case, the SBC continues to play the RBT using the previously agreed codec. **Root Cause:** There was a logical error in the code that was picking the currently active packet service profile to answer instead of honoring the modify. **Steps to Replicate:** Configuration: 1. Configure SBC to make a Basic A-B call. 2. Configure PSX with G711 and G729 in codecEntry and this Leg /other Leg configuration. 3. Configure LRBT, and attach to Ingress TG. Procedure: 1. Send an INVITE from UAC with G711. 2. Send an 180 from UAS, with no SDP. 3. Send an UPDATE from UAC, with G729. 4. Receive the 200 OK from INVITE from UAS.	The code is modified to address this issue. **Workaround:** None.
SBX-103771 | SBX-104825	2	PortFix SBX-103771: There are special characterss in DN hinders EMA display. **Impact:** The EMA does not display route with destination national containing special characters. **Root Cause:** The support for special characters was not available in EMA. **Steps to Replicate:** 1. In the SBC 7.2.4 R0, create a Route with Destination National containing special characters. 2. Upgrade to 8.2.4 R0. 3. After the upgrade, the EMA should display the route.	The code is modified to support special characters in the EMA. **Workaround:** The CLI can be used to view route details.
SBX-104247 | SBX-104644	2	PortFix SBX-104247: The resource memory congestion level 3 is approaching the threshold 90 sample 81. **Impact:** There was a SAM Process is leaking memory when AKA is being used. **Root Cause:** There was a SAM Process is leaking an AKA related structure when the code is handling an error case scenario. **Steps to Replicate:** The issue cannot be reproduced.	The code is modified to correctly free the AKA structure in all scenario. **Workaround:** There is no known workaround.
SBX-93898 | SBX-104516	2	PortFix SBX-93898: The "request sbx xrm debug command sec -stat gcid <gcid>" was not showing ENC and DEC details on the SBC SWe. **Impact:** This debug command in unhide section is not showing all the required fields populated in the SWe SBC. **Root Cause:** NP response is not framed in expected order to application layer. **Steps to Replicate:** Run the SRTP call and issue this debug command for internal use.	The code is modified so the NP Response is correctly framed in expected order to application layer. **Workaround:** This debug command is to see SSN field value with the RoC, all other details can be seen from show call mediastatus.

SBX-103599 | SBX-103893	2	PortFix SBX-103599; The SBC is sending multiple re-INVITEs to the ingress and egress leg during a 200OK of INVITE answered with Dialog-1. **Impact:** The SBC is sending multiple re-INVITEs to the ingress and egress side if the first forked leg is answering with a 200 OK. **Root Cause:** When the 200 OK is coming without SDP, we were taking last received SDP and that precondition attributes to further processing. **Steps to Replicate:** Precondition Transparency is set on both the Ingress and Egress Steps: UAC sends INVITE with Supported: precondition and SDP with precondition attributes. First forked UAS sends 183 with SDP with preconditions. Second forked UAS sends 183 with SDP with preconditions. First forked leg send 200 OK without SDP. Expected Behaviour: 1. The SBC transparently passes precondition attributes in SDP. 2. The SBC gets first forked 183 with SDP with preconditions. 3. The SBC forwards the 183 to ingress with preconditions. 4. The SBC sends an UPDATE to ingress and egress to complete precondition state. 5. The SBC forward second the 183 to ingress with preconditions. 6. The SBC sends an UPDATE to ingress and egress to complete precondition state. 7. The SBC forwards 200 OK and get ACK. 8. The SBC completes reINVITE-200-ACK towards egress.	The code is modified to address the issue. **Workaround:** None.
CHOR-6320 | SBX-105286	2	PortFix CHOR-6320: The UxPAD coredump observed on the media container while pumping 2X overload of G711U to G711U DSP (media transcoding disabled) call load. **Impact:** The SWe_UXPAD crash was seen during an overload transcode test in a 2 vcpu SWe deployment in the public cloud. **Root Cause:** Potential corruption in the packet buffers due to issues related to concurrency specifically in the 2 vcpu transcode overload scenarios. **Steps to Replicate:** 1. Configure a 2 vcpu instance. 2. Run 700 G711-G711 transcode sessions for overnight/long duration. 3. Check if there is any UXPAD/NP crash seen.	The code is modified to fix concurrency issues in transcode call scenarios in the 2 vcpu SWe deployments. **Workaround:** No workaround apart from avoiding overload scenarios for transcoded calls.
SBX-105182 | SBX-105414	2	PortFix SBX-105182: After the SBC receives RCODE = 2 from the DNS server, the SBC makes a strange query request to the DNS and subsequent new calls are rejected. **Impact:** When RCODE error received for the DNS query and no other servers were available, the record was never being deleted from cache and this remained as a RECORD in "RESOLVING STATE" that impacted further queries with this domain and resulted in call failures. **Root Cause:** This particular test scenario's was not covered during the testing feature. **Steps to Replicate:** 1. Setup with EDNS supported and DNS fall back disabled. 2. The single DNS server configured for the DNS Group. 3. The DNS Server configured to return RCODE Error 2 for SRV Query. 4. Setup a call that trigger NAPTR, SRV and A Query and the DNS Server responds with RCODE 2 for SVR. 5. Modify the DNS Server to return successful RCODE for SRV. 6. Make another call for the same domain. The call fails because the SRV record is in "RESOLVING STATE" in the cache.	The code is modified to delete cache entry (which is in "RESOLVING STATE") when the RCODE error is received. **Workaround:** NA

SBX-103255	2	Enhance the sbxPerf on the SBC for lesser resource consumption. **Impact:** The SBC performance monitoring tools like top and top2 at times take 20% of a CPU core there by reducing total available CPU resources for management activities on the SBC. **Root Cause:** The sbxPerf that contains list of tools such as top, mpstat, and iostat currently runs periodically without any linux value configured. This can cause these processes to get prioritized and scheduled ahead of other management processes such as ConfD and SSH. **Steps to Replicate:** Install fix build and ensure processes such as top, top2, mpstat sbxPerf are running with corrects value of 15 using the top command.	The code is modified so that priority of these processes are less compared to other management processes on the SBC. **Workaround:** None.
SBX-74155	2	The ACL rule is missing on the SBC in LD triggered switch-overs and link recovered after. **Impact:** When an IPACL rule is created that references an IP interface, but that IP interface has been down since the system started up, the rule is not successfully created. **Root Cause:** When an IP interface is failed on system startup, the system does not add that interface to the kernel. When an IPACL rule is added that references that IP interface, it fails to be added to the NP. **Steps to Replicate:** Start an SBC with an IP interface failed, that also has one or more IPACL rules that have been configured that reference that IP interface. Bring up the IP interface and logs will show the IPACL rules have been successfully added.	The code is modified to detect this situation and maintain a retry list. Once the IP interface comes up, it will retry the associated IPACL rules that were previously failed. **Workaround:** This issue can be worked around by having IPACL rules that do not reference the IP interface.
SBX-90854	2	There was a customer call forwarding MRF interaction failure on the receipt of an UPDATE. **Impact:** The SBC sends INVITE towards MRF upon receiving UPDATE from Egress End Point **Root Cause:** In some situations when there is delay in incoming PRACK request (In this situation PRACK from Ingress Endpoint), some internal logic of the SBC queues the SDP on ingress leg and let's SBC answer to egress, thereby unblocking the egress peer which can send a new offer using SIP UPDATE. This causes the SBC to send INVITE towards MRF, even before sending an UPDATE out towards the Ingress. **Steps to Replicate:** Configure the PSPs accordingly: 1. UAC sends Invite with AMR-WB, AMR, telephone-event. 2. UAS sends 183 with SDP with AMR-WB with 100rel. 3. UAC sends PRACK/200 OK. 4. UAS sends 180 without SDP without 100 rel. 5. PRACK for 180 is pending on Ingress. 6. UAS sends UPDATE with PCMU, telephone-event. Expected Results: ========== 1. Upon receiving an UPDATE with PCMU, the SBC will not auto answer towards UAS. 2. The SBC will wait for PRACK to be received from UAC, then will relay UPDATE towards UAC. 3. Based on answer in 200 OK (Update) from UAC, the SBC will send INVITE towards MRF for reserving transcoding resources.	The code is modified to ensure that SBC does not auto answer to egress. **Workaround:** None.
SBX-91111	2	The No Way Video after A/V calls is resumed after hold. **Impact:** No way video after audio video call is resumed using late media re-INVITE. **Root Cause:** The SBC does not send "sendrecv" in 200 OK to late media re-INVITE, instead sends the same datapath mode that was negotiated last - that is - inactive. **Steps to Replicate:** Setup an audio and video call. Put the call on hold by sending a=inactive in audio and video SDP. Then, send a late media re-INVITE to take the call off-hold. The idea is that the SBC will send SendRecv for audio and video in 200 OK and let the remote end choose if it wants to remain in hold or come out.	The code is modified to send sendrecv in other streams too when call is being "may be" resumed after hold. **Workaround:** Do not use late media re-INVITE to come out of hold.

SBX-92066	2	Observed a PRS process core dump "systemerror healthcheck timeout" **Impact:** A PRS coredump was found due to healthcheck timeout upon executing a CLI debug command **Root Cause:** The CLI debug command was taking a long time due to too many ACL entries resulting in a health check timeout. **Steps to Replicate:** 1. Add more than 1000 ACL entries 2. Execute below debug command: Run CLI debug command "request sbx xrm debug command acl\ -stat" **NOTE**: The debug commands are not available on customer sites.	The code is modified to process only 200 ACL entries to allow CLI to recover sooner. **Workaround:** As we do not run debug commands on customer sites, this error should not occur.
SBX-98843	2	There was a problem with management of the maxptime and ptime in the Direct Media mode. **Impact:** There was a problem with management of maxptime and ptime in the Direct Media mode. **Root Cause:** Generally, the SBC ignores the ptime value if only maxptime attribute is present in incoming SDP, If "sendPtimeInSdp" IPSP flag is enabled and peer is sending both ptime and maxptime, SBC is preferring maxptime value while sending ptime, The existing IPSP flag "sendPtimeInSdp" makes the SBC to send out a=ptime irrespective of what we receive from the peer. **Steps to Replicate:** 1. Do a basic call from A to B. 2. A sends ptime=20 and maxptime=40 towards the SBC. 3. An INVITE going out from the SBC should contain ptime=20 as we enabled both "sendPtimeInSdp" IPSP flag and "preferPtimeInSdp" TG flag.	A new flag "preferPtimeInSdp" is introduced under SBC CLI Trunk Group signaling. If this new flag "preferPtimeInSdp" is enabled, the SBC prefers ptime value received in a=ptime over a=maxptime in incoming SDP. This new flag "preferPtimeInSdp" needs be enabled in conjunction with existing flag "sendPtimeInSdp". If the SBC is configured to send a=ptime, then preferPtimeInSdp should be enabled on the incoming trunk and vice versa. **Workaround:** None.
SBX-103704	2	The RTP sourceAddressFiltering is not working (call leg dependency). **Impact:** The source address validation is not done if call flow does not involve NAPT learning. For calls that want source address validation but does not have NAPT enabled, the SBC would not validate the source address and end up forwarding the RTP packet to the other endpoint. **Root Cause:** There is no way for application to inform Network Processor to validate source if NAPT learning is not enabled. **Steps to Replicate:** Involves a CISCO MOH server but probably something else can be used.	The code is modified to validate source even when NAPT learning is not enabled to address the issue. **Workaround:** Enable NAPT learning for the call.
SBX-102827	2	The SBC5210 upgrade failure during Starting DB_RESTORE stage. **Impact:** An upgrade failure during Starting DB_RESTORE stage. **Root Cause:** Creation of foreign key fails on table packet_service_profile column CODEC_ENTRY_FK9, as it had "0" in one of its rows and dbimpl. codec_entry table did not have this value. **Steps to Replicate:** Upgrade a dump that has "0" in packet_service_profile.CODEC_ENTRY_FK9, it should be successful.	Before add the referential keys, the data is checked and ant value that is not there in parent table is nullified to address the issue. **Workaround:** None.
SBX-103669	2	Empty "Egress Local Signaling IP Addr" field in the CDR **Impact:** When an incoming call is routed out of the SBC but is then rejected by the SBC with cause 132 Module failure before a backwards response message has been received, the resulting attempt CDR has an empty "Egress Local Signaling IP Addr" field. **Root Cause:** The SBC currently populates the "Egress Local Signaling IP Addr" CDR field when it processes a backwards response message for the call, and as a result the field remains empty until a backwards response message is received and processed. **Steps to Replicate:** 1. Initiate a call by sending a valid INVITE to the SBC ingress TG to route towards the egress TG. 2. Once the INVITE is sent to egress by SBC, put the signaling port to egress out of service. 3. The SBC will clear the call by sending a 503 message towards egress. The resulting attemptCDR should have valid address in "Egress Local Signaling IP Addr" field.	The code is modified to populate the "Egress Local Signaling IP Addr" CDR field on sending out the egress INVITE message. **Workaround:** None.

SBX-104705	2	There was a memory leak on the glusterfsd. **Impact:** The OAM application cores. **Root Cause:** Memory leak is observed for the glusterfsd process, that is the brick process. The use of the "gluster volume heal info" function causes the process memory usage to increase and not go down afterward. **Steps to Replicate:** Ensure both Active and Standby OAM are running. Monitor glusterfsd memory usage on both nodes.	Use the "gluster volume heal statistics heal-count" command to determine the gluster bricks heal state to address the issue. **Workaround:** Reboot the OAM node.
SBX-103593	2	The SBC is ignoring Use Max Bitrate Only flag. **Impact:** The SBC is ignoring Use Max Bitrate Only flag. **Root Cause:** During Re-Invite answer processing, NrmaAdjustPeerT38MaxBitRate() routine is doing T38MaxBitRate adjustment based on packet size that is changing T38MaxBitRate value from 14400 to 4800. **Steps to Replicate:** Call Flow: 1. Do a basic call between UAC and UAS. 2. The UAS sends fax re-invite to UAC with T38MaxBitrate set to 14400. 3. The SBC sends Invite out with T38MaxBitrate set to 14400. 4. The UAC answers with T38MaxBitrate set to 14400 in 200OK. 5. The SBC sends out 200ok with T38MaxBitrate set to 4800. Actual Result: ------UAS(Re-Invite) ----------> SBC ----------> UAC T38MaxBitRate:14400 T38MaxBitRate:14400 -----UAC(200ok for Re-Invite) ----------> SBC ----------> UAS T38MaxBitRate:14400 T38MaxBitRate:4800 Expected Result: ------UAS(Re-Invite) ----------> SBC ----------> UAC T38MaxBitRate:14400 T38MaxBitRate:14400 -----UAC(200ok for Re-Invite) ----------> SBC ----------> UAS T38MaxBitRate:14400 T38MaxBitRate:14400	The code is modified to relay the T38MaxBitRate in SDP, which is received from peer for Direct Media calls. **Workaround:** None.

SBX-104560	2	The redirection NOA set wrong in the CDR. **Impact:** The "Redirecting Orig Cd Num - NOA" subfield of "Redirection Feature Spec Data" is not set correctly in CDR record if the the Redirecting Original Called Number - NOA value has been modified by PSX. **Root Cause:** The existing code was not updating the value for the CDR record based on route specific information returned from the PSX. **Steps to Replicate:** Test Setup ======== 1. Test requires call routing through the PSX. Routing on PSX, setup to route incoming call through routing label with two routes: - route 1, through local egress trunk group 1 on SBC to UE2. - route 2, through local egress trunk group 2 on SBC to UE3. 2. On egress trunk group 1 only, associate a DM/PM rule to change the "Number Type" to International for "redirecting Original Called Number". 3. Set the crankback profile to enable attemptRecordGeneration and add reason 41 (503 is mapped to 41 in default SIP to CPC mapping profile) set profiles callRouting crankbackProfile default attemptRecordGeneration enabled reason 41 Test Procedure ============ 1. Send INVITE to the SBC ingress, INVITE should include a diversion header e.g. Diversion: <sip:+4969667740185@xxx.xxx.xxx.xxx>;privacy=off;screen=no;reason=unknown;counter=1 2. Call is routed using route 1, respond from first egress with 503 Service Unavailable 3. Call is re-routed using route 2, respond from second egress with 503 Service Unavailable 4. Check the CDR records for call on the SBC that should have two attempt records - a. ATTEMPT1 - should have "Redirection Feature Spec Data" that has subfield 22 "Redirecting Orig Cd Num - NOA" as 3 (Unique International Number), because the number was updated by PSX to international. b. ATTEMPT2 - should have "Redirection Feature Spec Data" that has subfield 22 "Redirecting Orig Cd Num - NOA" as 2 (Unique National Number), because the number was not updated by PSX	The code is modified to populate the CDR value from the route specific data returned from PSX. **Workaround:** None.
SBX-103986	2	There was an incorrect RTP time stamp in the SBC packet capture. **Impact:** After an SBC upgrade to V09.01.00R001, RTP/RTCP time stamp in the SBC packet capture shows the year 2036. **Root Cause:** Present logic was not considering the edge cases while checking the last modification time of the NTP log. **Steps to Replicate:** 1. Configure a remote syslog server: set oam eventLog platformRsyslog linuxLogs ntpLog enabled set oam eventLog platformRsyslog servers server1 port 10514 protocolType udp remoteHost <remote host ip> com set oam eventLog platformRsyslog syslogState enabled com 2. Create a second dummy NTP server (just to trigger some logs to be written to ntp.log): set system ntp serverAdmin 1.2.3.4 com 3. Delete the dummy NTP server: del system ntp serverAdmin 1.2.3.4 com 4. Wait at least several seconds. 5. Repeat steps 2 and 3.	The code is modified for the edge case of NTP log last modification time. **Workaround:** None.

SBX-94798	3	The MS Teams with FLRBT enabled hangs the call. **Impact:** When the Force Local Ringback Tone is applied on a call that has been through SIP replace followed by SIP refer procedure, and the final trunk group has downstream forking enabled. The final 200 OK response may be queued indefinitely, meaning the call does not get completed. **Root Cause:** Interactions between Force Local Ringback Tone, multi-party and downstream forking. **Steps to Replicate:** 1. Make a SIP to SIP call. 2. A calls B. 3. B' replaces B. 4. B' refers to C. 5. The trunk for A has Force Local Ringback Tone applied. 6. The trunk for C has downstream forking enabled. 7. C responds with 180 with no SDP, 183 with SDP, then 200 OK.	The code is modified to prevent the queuing. **Workaround:** None.
SBX-99306	3	The SIPCM (SAM) deadlock reported on SNMP request. **Impact:** The SAM Process cores when getTlsStatus command is executed. **Root Cause:** The issue is because when fetching the TLS Status, we were trying to access sessData that was no longer valid. **Steps to Replicate:** Execute getTlsStatus command when running TLS load. SAM process cores randomly.	The code is modified to fetch the status from socketPtr instead of sessData. **Workaround:** None.
SBX-100086	3	The sbxAutoBackup.sh changes for AWS SWE. **Impact:** The Cloud SBC uses default system name 'vsbcSystem' when creating system backups, making it difficult to distinguish between setups. **Root Cause:** The Cloud SBC configuration file backup logic uses the system name to create the back up file instead of the specific name. **Steps to Replicate:** Run /opt/sonus/sbx/scripts/sbxAutoBackup.sh on the SBC running in a cloud (e.g. AWS) that has SystemName configured too something specific in user-data.	Use the actual system name (configured in user-data) in the configuration backup filename to address the issue. **Workaround:** None.
SBX-91016	3	Unable to see the signaling messages on the PKT log file. **Impact:** The Packet capture does not work properly for pkt ports. **Root Cause:** The version of libpcap0.8 library in Debian9 had a defect that resulted in the capture not working. **Steps to Replicate:** 1. Login to the SBC and run a basic call configuration. 2. Create a signaling packet capture filter: set global callTrace signalingPacketCapture state enable devices pkt0 0. 3. Run the SIPP calls. Expected Results: 1. The SBC should capture all the signaling messages on the pkt0 port in a PKT file under the gsxlog directory.	Update the libpcap0.8 to a newer version to address the issue. **Workaround:** None.
SBX-74709	3	The SBC REST API. pam phase authorization failed to login through a PAM: timeout **Impact:** Too many requests on the REST API interface causes 401 error. **Root Cause:** Issue with third party tool ConfD that is used for configuration management. **Steps to Replicate:** 1. Send REST API requests for long duration. 2. Open some CLI session for some time to cause max session limit. 3. REST APIs start failing with 401 error due to session limit, as expected. 4. Close the CLI sessions. 5. REST APIs keep failing, even after keeping CLI sessions under max limit.	The code is modified to fix the issue. **Workaround:** None.

SBX-101408	3	The SIPREC was not working. No request sent to recorder. **Impact:** Without this fix, SBC is generating INVITE towards the SIPREC SRS with bad format on SDP header line 'label'. The 'label' header is missing the CR in the CRLF line break. **Root Cause:** The code that formed the SDP header line "label" does not add CR character for CRLF line break. **Steps to Replicate:** Make a call that would match the configured SIPRec criteria and thus triggering a SIPRec session for the corresponding Communication Session.	The code is modified to add CR character for CRLF line break, for SDP header line "label" . **Workaround:** None.
SBX-104324	3	The reenableOsAccount silently sets an account expiration to 30 days. **Impact:** Using the reeanbleOsAccount will add account aging to any OS account. **Root Cause:** The logic does not take into account the state of OS account aging or if OS account aging should be applied (e.g. root). **Steps to Replicate:** Run with an OS account aging enabled: 1. Test root: a. ReeanbleOsAccount for user root. b. Check no aging has been applied at OS level: chage -l root. 2. Test the Confd user: a. Create user through CLI. b. ReeanbleOsAccount for this CLI user. c. Check no aging has been applied at OS level: chage -l <CLIUser>. 3. Test OS user with a password: a. Create OS user with a password. b. Disable and then Enable OS account aging state. c. ReeanbleOsAccount for this OS user. d. Check correct aging has been applied at OS level: chage -l <OSUser>.	The code is modified in the OS account aging is enabled and is applied to the account. **Workaround:** None.
SBX-97555	2	The active OAM node for the Signaling SBC generates header-only ACT files and pushing it to the billing server, where the OAM node should be responsible for the configuration only. **Impact:** The active OAM node generates header-only ACT files and pushing it to billing server. **Root Cause:** The SBC does not check whether it is OAM node or Managed VM while generating ACT files. **Steps to Replicate:** Spawned a Nto1 OAM node, check whether .ACT files exist or not. Restart active Node, Check if any .ACT file gets created. Restart the current Active again (assigned role Standby) and check whether any .ACT file is present on OAM node or not.	Check whether VM is OAM before creating the ACT files to address the issue. **Workaround:** None.
SBX-102501	2	The SBC fails to relay embedded header in Contact of 3xx with statusCode3xx relay enabled **Impact:** The SBC fails to relay embedded header in Contact of 3xx with statusCode3xx relay enabled **Root Cause:** The code required to send the embedded part in contact of 3xx was not present **Steps to Replicate:** 1. Configure the SBC for A to B call. 2. Enable the flag statusCode3xx on egress TG IPSP. 3. Send an INVITE from UAC. 4. Send 300 Multiple Choice from UAS with below Contact header that has embedded headers.	The code is modified so the contact header transparency is set in the relay 3xx scenario that is now being changed to full contact header transparency and set the SIP_HEADER_URI_HEADERS so that the embedded contact header is transparently passed in the 3xx. A new header type is introduced that is set only in the relay 3xx case to send the entire contact header transparently. **Workaround:** None**.**
SBX-102234	2	The SubsystemAdmin filter affects calltrace (TRC) logging showed useless logs. **Impact:** After creating then deleting an entry in the oam eventLog subsystemAdmin, the original behaviour is not restored. INFO level events for that subsystem are no longer logged, even if the oam eventLog typeAdmin filterLevel is info. **Root Cause:** Deleting an entry in oam eventLog subsystemAdmin does not restore settings back to default. **Steps to Replicate:** 1. Create an entry for a subsystem in the oam eventLog subsystemAdmin table. 2. Delete the entry.	The code is modified to process to deleted the oam eventLog subsystemAdmin entry so that settings are put back to default values. **Workaround:** None.

SBX-86090	2	Our SIPREC implementation is prone to failure to record a stream and to tear down the SRS call leg when SRS (SIP Recording Server) sends a re-INVITE to SBC **Impact:** SIPREC handling had race conditions issues in the scenario where a RE-INVITE was received on the main call and also RE-INVITE was received from SRS server at the same time. This resulted in recording failure and the SBC sent out BYE towards SRS. **Root Cause:** This race condition of RE-INIVITE from the main call end point and SRS server simultaneously was not handled on the SBC. **Steps to Replicate:** 1. Make a SIPREC call. 2. Send RE-INVITE with codec change/hold on main call (either from UAC or UAS) this triggers a RE-INVITE towards SRS. 3. SRS also sends RE-INVITE at the same time when SBC receives 200 OK for main call RE-INVITE.	The RE-INVITE triggered/sent towards SRS due to the main call RE-INVITE is queued in the situation where the SIPREC leg is in middle of processing the RE-INVITE that was received from the SRS. The queued RE-INVITE would be sent once the RE-INVITE transaction received from the SRS was completed. **Workaround:** The SRS can avoid sending immediate hold RE-INVITE if no media is observed on SIPRec leg.
SBX-104093	2	The EMA codec entry screen was not usable. **Impact:** The EMA codec entry screen was not usable. **Root Cause:** The method call place mismatched. **Steps to Replicate:** 1. Log into EMA. 2. Navigate to **Profiles** > **Media** > **Codec Entry** 3. See that the screen is working correctly.	The code is modified so the EMA codec entry screen is placed at the appropriate position. **Workaround:** None.
SBX-74907	2	A SIPREC Codec issue. **Impact:** Without this fix, the wrong codecs are negotiated with SRS when communication sessions is renegotiated. **Root Cause:** Because of wrong conditions in code, the codec information that is to be sent towards SRS is fetched from peer packet service profile rather than active service profile from the communication call leg. **Steps to Replicate:** 1. The SBC receives INVITE with G711A, G711U 2. Egress leg responds with A law and RTP stream is A law. 3. The SBC sends an INVITE to SIPRec server with G711A law and SIPRec servers responds with A law. 4. Egress leg sends re-INVITE and changes the order of codecs, G711U and G711A respectively. 5. The SBC relays the re-INVITE to ingress peer with G711U, G711A respectively and ingress peer responds with G711A. 6. The SBC was sending re-INVITE with G711U codec to SIPRec Server. With this fix, SBC now sends re-INVITE with G711A codec to SIPRec server.	The code is modified to fetch correct codec information from the communication session and the same is sent in recording session. **Workaround:** None
SBX-102993	2	The "numMatch notmatch" gets auto converted to "numMatch match" when SMM profile is modified/saved from GUI **Impact:** The "numMatch notmatch" gets auto converted to "numMatch match" when SMM profile is modified/saved from GUI **Root Cause:** The numMatch field was not there in the EMA. **Steps to Replicate:** 1. Navigate SipAdaptorProfile screen. (ProfilesSignallingSipAdaptorProfile). 2. Create profile with the selection numMatch field. 3. Create profiles with all possible values. 4. Here the numMatch field was newly added. 5. Verify whether all field values are coming properly or not.	The code is modified to address the issue. **Workaround:** None.
SBX-103692	2	The SWe application will not start: The memory mismatch after a AWS instance restart. **Impact:** The standby SBC shuts down if the memory product capability mismatches with the active SBC. **Root Cause:** The SBC checks for a minimum required memory with the memory allocated to peer and it should be either equal or greater than the peer SBC. **Steps to Replicate:** Launch the SBC HA pair on AWS to see if the memory allocated to the standby SBC is lower than an active SBC.	The code is modified to change the memory from 'Minimum required' to 'Informational' to not shut down the app in case of a mismatch and only raises a trap. **Workaround:** Try rebooting in case memory allocated to standby the SBC is lower than the active SBC.

SBX-104552	2	After a switchover, the MRFP does not send a Goodbye packet for the Text stream. **Impact:** When a call is using T140/TTY interworking, after a switchover RTCP bye is not sent toward the T140 stream endpoint. **Root Cause:** In a T140/TTY interworking, the resource for T140 stream is not mirrored properly to standby causing deactivating does not work after a switchover. **Steps to Replicate:** 1. Make call with T140/TTY interworking (for example, AMR-WB+T140 - PCMU). 2. Once call is established, switchover. 3. After a switchover was successful, end the call and see that RTCP bye is sent properly to T140 stream.	The code is modified to mirror resource correctly for T140 stream in T140 /TTY interworking. **Workaround:** None.
SBX-104563	2	The SBC is not updating the DNS servers order in DnsServerStatistics on deleting and creating a fresh DNS Group. **Impact:** The SBC was showing the incorrect DNS Servers Index in DnsServerStatistics command "show table addressContext default dnsGroup <dnsGroupName> dnsServerStatistics " when the DNS Servers were deleted and re-created in a different order with the same server IPs. After creating 128 DNS Servers with different unique IPs are and then deleting some of them such that the total number of DNS Servers is less than 128, no new DNS servers created post the delete operations shall have the corresponding statistics information, even though the total number of servers is less than 128 on the system. As an example, if on the SBC we create a DNS Server with IP1 and then delete it and then proceed on to repeat the create and delete operations with different IPs say IP2 to IP128, then from the IP128 onwards, no statistics shall be displayed, even though there is only one DNS Server on the system. **Root Cause:** The DNS Server Statistic blocks are not deleted when the DNS Servers are deleted and continues to remain hashed with the IP with that it was created. **Steps to Replicate:** 1. Configure the DNSGROUP. 2. Add the 1st DNS server with IP1 to DNSGROUP. 3. Add the 2nd DNS server with IP2 to DNSGROUP. 4. Check the DnsServerStatistics. show table addressContext default dnsGroup <dnsGroupName> dnsServerStatistics 5. Delete the DNSGROUP. 6. Configure the DNSGROUP. 7. Add the 1st DNS server with IP2 to DNSGROUP. 8. Add the 2nd DNS server with IP1 to DNSGROUP with weight1. 9. Check the DnsServerStatistics. 10. The IP2 should have 3 as Index and IP1 should have 4 as index in dnsServerStatistics.	The code is modified to delete the DNS Server Statistics block and remove it from the IP hash when the DNS Server is deleted. **Workaround:** None.
SBX-103732	2	The AddressSanitizer: heap-buffer-overflow on address 0x61d001429c18 at pc 0x556c876cf74c bp 0x7fb14f64fab0 sp 0x7fb14f64f260 READ of size 3488 at 0x61d001429c18 thread T21 in the SAM Process. **Impact:** In a D-SBC environment while processing the remote media data command message, the SAM process could read off the end of the received message. Reading off the end of the allocated message block could, in the worst case, result in a coredump. **Root Cause:** The SAM process was assuming that the size of the received message was larger than it actually was and this resulted in reading off the end of the received message buffer. In most cases, this does not cause a problem but in could potentially result in a coredump if the associated buffer is at the end of the addressable memory space. **Steps to Replicate:** Run the RFC4117 test case for audio transcoding and video relay.	The code is modified to not read off the end of the received memory block. **Workaround:** None.

SBX-102175	2	The HA SBC Admin Connection failure issue within sometime for the ASAN build. **Impact:** In an HA setup, the standby SCM process can read off the end of a memory block. Reading off the end of allocated memory blocks can cause unexpected behaviour and in the worst case, it could result in coredumps. This problem only impacts the standby server so will not be service impacting. **Root Cause:** While making P-Asserted-Id header information redundant between active and standby, the standby was reading off the end of the allocated memory buffer because the active instance had passed over a bad data length value for P-Asserted-Id header. **Steps to Replicate:** Run a call load where the INVITE messages contain P-Asserted-Id header in an HA setup.	The code is modified to correctly format the P-Asserted-Id header information with valid length when sending it to the standby to avoid the standby accessing invalid memory. **Workaround:** None.
SBX-105280	2	The CPX Process had a memory leak for single call on the OAM node. **Impact:** The CPX process can leak small amounts of memory when creating/modifying the SNMP configuration. **Root Cause:** While processing the SNMP configuration commands, the SBC was creating the temporary internal memory blocks to read and write information from/to the CDB. But it was not freeing up this memory at the end of the configuration action. **Steps to Replicate:** Modify the SNMP configuration.	The code is modified to correctly free the temporary memory allocated during the configuration process. **Workaround:** None.
SBX-105542	2	Fix the Customer Telecom coverity issues. **Impact:** While processing the SUBSCRIBE messages, the coverity tool has highlighted that the code could dereference a pointer that is potentially null. Although no bad behaviour has been observed during testing, there is a small chance that it could result in coredumps if the pointer really was null. **Root Cause:** Based on other validation in the code, the coverity highlighted that some legs of code could result in accessing a pointer that might be null. Derefencing null pointers can cause unexpected behaviour and in the worst case coredumps. **Steps to Replicate:** Run various SUBSCRIBE related test cases.	The code is modified to validate that the pointer is not null before using it to avoid any potential issues/coredumps. **Workaround:** None.
SBX-91127	2	The leaksanitizer had an CpxAaaGetNextEntry. **Impact:** While processing the requests to display the user information /status, the Cpx process was leaking memory. **Root Cause:** While processing the requests to display user information /status, the Cpx process had to allocate the internal memory blocks to collect information from CDB and was not freeing up this memory at the end of the request. **Steps to Replicate:** From the CLI, run commands to request user information.	The code is modified to free up the memory at the end of the processing request. **Workaround:** None.
SBX-105389	2	De-reference after a NULL check and de-reference the NULL return value. **Impact:** The coverity scanning tool identified a potential edge case scenario, where the lawful intercept code could potentially access a NULL pointer leading to unexpected behaviour and potentially a coredump. **Root Cause:** While the code was performing X2 peer status updates, it retrieved the peer information from a hash table but did not verify that the pointers inside the record it retrieved were valid. It would be an extreme error case for this to result in reading of a null pointer and would likely need to be due to another problem. But coverity highlights it as an edge case issue to fix up. **Steps to Replicate:** Run test cases for lawful intercept using packet cable V2.0 configuration.	The code is modified to validate the pointer is not null before using it and avoid any error scenarios. **Workaround:** None.

SBX-100225	2	The AddressSanitizer: detected heap-use-after-free in UasProcessMsgCmd on address 0x623000187198 at pc 0x5623cc7b3b42. **Impact:** The SCM process is accessing memory after it has been freed during the timer expiry handling when there is no response to an OPTIONS message that was triggered due to debug optionsPing using an FQDN. Accessing memory after it has been freed can cause unexpected behavior and in the worst case, this potentially causes coredumps. Ex:"request addressContext default cmds optionsPing peerFQDN bats3.gsxlab.com peerPort 14090 sigPort 2 transport udp" **Root Cause:** The SIP dialog memory block was being removed in two places while handling the timeout for the debug optionsPing command, which could result in unexpected behaviour and potentially result in coredumps. **Steps to Replicate:** 1. Run debug optionsPing command "request addressContext default cmds optionsPing peerFQDN bats3.gsxlab.com peerPort 14090 sigPort 2 transport udp" 2. The OPTIONS message will be sent out. 3. Let the options timeout. (do not send any response).	The code is modified to address the issue. **Workaround:** Do not use this debug command, or use it with an IP instead of an FQDN.
SBX-105591	2	Observed that PRS process heap buffer overflow issue on 9.2 ASAN build 63 **Impact:** The BRM process was accessing memory after it had been freed. As the memory is being read immediately after being freed, then it is unlikely this would cause a problem. **Root Cause:** If the BRM process received an unexpected message, then it was trying to print a debug message to indicate the message type. However, the message had already been freed up because it was unexpected. This was observed on the standby server and generated at the point of switchover. **Steps to Replicate:** Run a normal call load and perform switchovers.	The code is modified to collect the message type information before the message is freed so that the debug log content can be safely generated without accessing freed memory. **Workaround:** None.
SBX-103650	2	The SCM Process cores when the targets set for OPTIONS/MESSAGE. **Impact:** Without this fix, the SBC will core dump when the Out Of Dialogue messages like OPTIONS/MESSAGE are intercepted. **Root Cause:** Double free of a data structure is causing the code dump. **Steps to Replicate:** 1. Provision packet cable 2.0 Targets corresponding to the out of dialogue OPTIONS that will be sent to the SBC. 2. Send the OPTIONS to the SBC.	The code is modified to avoid double freeing of the corresponding data structure. Also, addressed couple of memory leaks concerned with the same data structure in error cases such as ARS blacklisting. **Workaround:** None.
SBX-103788	2	The LeakSanitizer: detected memory leaks in CpxAppProcess. **Impact:** Small memory leak when making configuration changes to the GW signaling port. **Root Cause:** The configuration logic was reading the interface group name from CDB into a temporary local variable in order to perform validation logic but never freed up this memory at the end of the validation. **Steps to Replicate:** This issue is highlighted in the engineering lab when performing GW sig port configuration changes on an ASAN enabled build.	The code is modified to correctly free the temporary memory to avoid the leak. **Workaround:** None.
SBX-105412	2	The MRFP: CE_2N_Comp_CpxAppProc leak for port SWO (BFD). **Impact:** There was a small memory leak during the configuration of packet port with BFD configuration associated. **Root Cause:** The configuration code was reading information from the CDB and storing information in an internal memory block but not freeing it up. **Steps to Replicate:** With a BFD configuration on the SBC, disable and enable the pkt port by setting mode OOS and state disabled and then enable the pkt port again.	The code is modified to correctly release the internal memory block at the end of the configuration action. **Workaround:** None.

SBX-105496	2	Fixing the NRMA coverity issue CID:11149. **Impact:** The coverity scanning tool identified a potential code leg where a null pointer could be dereferenced and could potentially result in a coredump, although not observed in internal testing. **Root Cause:** While trying to allocate resources for PCMU to PCMA call where the ingress leg is being tapped, there is a possibility the code could access and invalid pointer resulting in unexpected behaviour and in potential coredumps. **Steps to Replicate:** This part of the code could be triggered for PCMU to PCMA call where the ingress leg is being tapped.	The code is modified to verify the pointer is not NULL before trying to use it to avoid potential coredumps. **Workaround:** None.
SBX-105200	2	The AddressSanitizer: detected heap-use-after-free on address 0x6080002177a0 at pc 0x55a942cce5b1 bp 0x7fb90b2df190 sp 0x7fb90b2df188. **Impact:** There were two types of issues identified in this Jira: 1. There was a memory leak when putting a virtual media gateway in service. 2. The MRFP is accessing memory after it is freed while cleaning up a call following an internal resource allocation failure. Accessing memory after it has been freed can have unexpected behavior and in the worst case result in coredumps. **Root Cause:** 1. The MRFP was allocating internal memory while performing validation of the request to put a virtual media gateway inservice, but the memory was not being freed up at the end of the configuration action leading to a small memory leak. 2. In case of internal call failure, the call data was being deleted but the memory was being access later on in the clean up procedure. **Steps to Replicate:** 1. Configure a virtual media gateway in service. 2. Configure the MRFP without licenses and then try to make some calls.	1. The code is modified to free the memory at the end of the configuration action. 2. The code is modified to no longer access the call data after is free. **Workaround:** None.
SBX-104118	2	The LeakSanitizer detected memory leaks in the SCM Process. **Impact:** While relaying REGISTER messages, the SBC may leak memory blocks allocated to hold the record-route header information. **Root Cause:** The SBC allocates memory blocks to hold the contents of the record-route headers in the REGISTER message. But if the record-route header information is associated with the SBC IP address, then the SBC does not correctly free up the memory blocks causing a leak. **Steps to Replicate:** Run test cases for stateless REGISTER relay call scenarios where the IP information in the record-route header is the SBC's IP.	The code is modified to correctly freed up memory allocated to store the record route header information. **Workaround:** None.
SBX-105850	2	The MRFP failed to come up after an sbxstart. **Impact:** At startup of the SBC, there is a possible race condition where the SBC processes may go for an additional restart before they come up and restore the configuration. data. **Root Cause:** The race condition in the code between threads. **Steps to Replicate:** Installation and startup on the various platforms.	The race condition in setting some common variables is avoided by using static path of binaries to address the issue. **Workaround:** None.

SBX-103626	2	Due to the Adaptive Codec Change, the MRFP does not disable the text stream although there is conflict between the payload types that the non audio and text streams use. **Impact:** In a audio and T140 call setup, with Adaptive Codec Change enabled and the MRFP does not disable the text stream when there is conflict between the payload types that the audio and text streams use. **Root Cause:** In the Adaptive Codec Change handling, the code does not validate if the payload type used in the T140 stream are in conflict with payload types being used in the audio stream codecs. As a result, the T140 stream is created in the media plan that should be disabled in this scenario. **Steps to Replicate:** 1. Enable Adaptive Codec Change in the VMG configuration. 2. Setup a call audio and T140 media streams from both call terminations: A- side AMRWB and text 140 to B side, AMR, text T140, and Telephone event. 3. At the mid call, send a Re-Invite to change B's side to AMRWB, T140 and Telephone Event with its payload type is the same as the T140's payload type. 4. Verify that MRFP should disable the T140 stream by setting the t140 stream port number to zero in the reply to MGC(C3).	The code is modified to check the conflict for T140 payload types against the payload types being used in an audio stream, and reject T140 stream when a conflict is found. **Workaround:** None.
SBX-105039	2	The SBC fails to perform Alert-Info to PEM interworking when the relayPemState is disabled on the ingress. **Impact:** The SBC fails to perform Alert-Info to PEM interworking when the relayPemState flag is disabled on the ingress TG. **Root Cause:** The relayPemState flag implementation was not considered for Alert-Info to PEM Interworking scenarios. **Steps to Replicate:** Configuration: 1. The relayPemState flag is disabled on the Ingress TG. 2. The iToPemInterworking flag is enabled on the Egress IPSP. 3. The acceptAlertInfo flag is enabled on the Egress IPSP. 1. The UAC sends an Invite with the SDP with PEM: supported to the SBC. 2. The UAS sends 180 without the SDP with an alert-info as rt to the SBC. 3. The SBC should interwork the alert-Info to PEM and insert PEM: inactive while sending 180 responses towards UAC.	The code is modified to consider the Alert-Info to PEM Interworking scenarios when the relayPemState flag is disabled. **Workaround:** None.
SBX-65509	2	The preferred payload number was not used for either dtmf or amrwb when the "different2833PayloadType" transcode option is enabled. **Impact:** The preferred payload number was not used for either dtmf or amrwb when the "different2833PayloadType" transcode option is enabled. **Root Cause:** Both the AMR-WB and dtmf do not use 101, as 101 was being neglected and thinking the other one was using it. So at the end, it was not being considered and was not being populated. **Steps to Replicate:** Make a SIPP call using AMR-WB codec with dmtf enable different2833palyloadtype flag. enable honorSdpClockRate flag. set preferredRtpPayloadType as 101 set preferredRtpPayloadTypeForDtmfRelay 101 Check for the Preferred payload number.	The code is modified to scan even the workingDynamicPtSet and verify that 101 is not being used and is considered. **Workaround:** The workingDynamicPTSet represents a more accurate information w.r.t the PTs used. As a result, that condition is being added to scan workingDynamicPtSet along with peer PSP and Route PSP.
SBX-104471	2	There was a CE_node error "glusterSetup.sh Abort: Mount is in bad state!!" **Impact:** A glusterSetup.sh script error log showing in CE_Node log file. **Root Cause:** A glusterSetup.sh script error text is printed to the terminal. **Steps to Replicate:** 1. Shut down the Standby OAM. 2. Ensure there is no glusterSetup.sh log appear in CE_Node log file on managed node.	The error text already captured in two separate log files, so remove the output to terminal to address the issue. **Workaround:** None.

SBX-101406	2	Implement SAN validation for cert authentication in VNFR REST Server **Impact:** The VNFM request did not have SAN validation in addition to a cert chain verification. Now, the SAN validation checks against IPv4 and IPv6 both if present in userData. **Root Cause:** The SAN validation was not implemented. The SAN validation used to work only in mode(either IPv4 or IPv6) depending upon the SBC instantiation mode. **Steps to Replicate:** 1. Bring VNFR(running HTTPS) from VNFM GR. 2. Perform a successful reassignment. 3. Do a sbxrestart. 4. Again perform a successful reassignment. 5. Bring up a dual stack VNFM, and spawn IPv4 and IPv6 SBC. 6. Register VNFR successfully in a simplex VNFM.	Implemented SAN validation using GnuTLS that is also used for cert chain verification. Loading both IPv4 and IPv6 from userdata addresses the issue. **Workaround:** No workaround.
SBX-94760	2	The cinder volume detach/attach required a reboot from Openstack to bring up all the functioning related to the SBC. **Impact:** In the case of Openstack, if cinder volume is detached from the running the SBC instance, it does not cause the SBC system to shutdown properly. **Root Cause:** The shutdown triggered on the volume detach from a running instance was not going through successfully due to failure to run abnormal reboot command. **Steps to Replicate:** Test cinder volume detach from a running instance and ensure the node goes for a reboot and if running on active, should switchover to standby successfully.	The code is modified to update the command to forcefully reboot the node on volume detach from a running instance. **Workaround:** None.
SBX-93790	2	A TEAMS user was unable to resume the call when transfer is failed, when the call is initiated in beginning by PSTN user. **Impact:** During a Refer, if the transfer target sends early answer in 18x but then rejects the call, the SBC fails to resume the previously active call. **Root Cause:** During call transfer, after tone play, while processing early answer in 183, the SBC wrongly freed the previous cut-thru context and instead retains the previously activated tone context (for A-B call). As a result, after transfer target rejects the call, the SBC attempts to resumes the previously active call (A-B) which fails due to unavailability of correct context. **Steps to Replicate:** 1. PSTN1 to TEAMS call TEAMS transfer call to PSTN2 PSTN2 rejects the call TEAMS resume the call 2.PSTN1 To TEAMS call TEAMS transfer call to PSTN2 PSTN2 does not answer the call TEAMS resume the call	The code is modified to retain the previously activated cut-thru context and free the previously activated tone context if current tone context is more recent. **Workaround:** No
SBX-104331	2	Observed the "NrmUpdateLicensesForXferFeatureType cant get origGCID" MAJOR Logs on the 5400 Platform while running a call with Multiple INVITE Replace. **Impact:** The Call Pickup logs were incorrectly printing a major error event. **Root Cause:** The Call Pickup logs were incorrectly printing a major error event. **Steps to Replicate:** None.	The code is modified to address the issue. **Workaround:** None.

SBX-104738	2	The outputAdaptor profile rule gets applied after the clearDB. **Impact:** The SMM rule was not applied after the upgrade from 8.2 or 9.0 or 9.1 to 9.2, even the same issue is observed during restart or switchover. **Root Cause:** The SMM rule was not applied due to wrong path in the switchover scenario. **Steps to Replicate:** Configure the SMM profile in the SBC. Perform any of the of the below steps. 1. Restart the SBC. 2. The SBC performs a switchover. 3. Upgrade from 8.2/9.0/9.1 to 9.2.	The code is modified to address the issue. **Workaround:** ClearDB and load the configuration.
SBX-95677	2	The SBC is not feeding the delayed RBT on monitoring a failure in a late media passthrough scenario in the CLOUD ISBC and SWE ISBC. **Impact:** The SBC is not feeding delayed RBT on monitoring the failure in a late media passthrough call. **Root Cause:** The fix for the SBC was not feeding delayed RBT on the monitoring failure in a late media passthrough scenario was applicable only when bToneAsAnnc flag is enabled. **Steps to Replicate:** Procedure: 1. An INVITE is received without SDP and no "PEM: supported" from the UAC. 2. The UAS sends the 183 with SDP and no PEM having PCMU, AMR. 3. The UAC send PRACK with SDP PCMU,G729 and UAS sends 200 OK for PRACK. 4. The UAS sends an authorized RTP. 5. The UAS sends 180 without SDP and no PEM. 6. The UAC send PRACK and UAS sends 200 OK for PRACK. After a RTP Monitoring failure, the SBC should play the tone.	The code is modified to address the issue. **Workaround:** None.
SBX-104136	2	Unable to login to the CLI session. **Impact:** The SWe Active profile configuration may cause a password change commit to hang. **Root Cause:** The Internal Configuration change related to sweActiveProfile leaves the changes in the candidate database. This causes another commit from the SM Process deadlock, as sweActiveProfile change subscription needs the SM Subscribers acknowledged. **Steps to Replicate:** This cannot be recreated through User Interfaces. This was an internal error condition.	The code is modified to revert the changes from the candidate database, if the sweActiveProfile commit fails. **Workaround:** None.
SBX-102958	2	The Audit Compliance issues are found in the MRFP Setup. **Impact:** The Nessus Scan with the CIS Plugin shows compliance failures on the SBC. **Root Cause:** The failures were due to a missing a user directory and bad file permissions. **Steps to Replicate:** Run the Nessus scan with the same policy and verify that the failed compliances do not exist.	Below changes are made to meet the CIS requirements. 1. Set nologin shell for cwagent 2. Change remoteExecution.log file permission. **Workaround:** None.
SBX-103273	2	Dual NUMA support in the SWe. **Impact:** The SWe does not come up in the VMs having multiple NUMA nodes except for the signaling traffic profile (SLB, S-SBC, SO-SBC). **Root Cause:** Due to a deliberate software restriction to not allow multiple NUMAs, the issue was shown. **Steps to Replicate:** 1. Configure a KVM instance with the dual NUMA and install in Non-Gold/Non-GPU setup. 2. Let it come in default traffic profile. 3. Verify that the SBC would come up fine without any HostCheck errors.	The code is modified to allow multiple NUMA irrespective of the personality and profile. **Workaround:** None.

SBX-103627	2	The BFD status is not up for the MGMT port (the BFD packets are seen though the LDG state is disabled). **Impact:** Even after disabling Link Monitor on the MGMT port, the BFD packets are still seen on the MGMT port. **Root Cause:** The issue was that when state is disabled and the BFD session was deleted. A timer is started so the expiry initiates a BFD session. **Steps to Replicate:** 1. Create BFD session for MGT port. 2. Check the status of BFD session. 3. Disable the BFD session. 4. Observed the BFD packets even when the BFD session is disabled.	The code is modified to check for the Link Monitor state before initiating the BFD session. **Workaround:** None.
SBX-103489	2	The LeakSanitizer: detected memory leaks at the confd_malloc. **Impact:** The small memory leak during the configuration of lawful intercept server. **Root Cause:** The configuration code was reading information from the CDB and storing information in an internal memory block but not freeing it up. **Steps to Replicate:** Create a lawful intercept server and make configuration changes.	The code is modified to correctly release the internal memory block at the end of the configuration action. **Workaround:** None.
SBX-103387	2	The Video NAT learning is failing on the D-SBC cloud. **Impact:** The Video NAT learning failed in the D-SBC. **Root Cause:** On the D-SBC, NAT learning for video stream was not processed successfully and as a result caused the video packets to be dropped by the SBC. **Steps to Replicate:** 1. Configure the SBC for an Audio and Video call. 2. Enable the Signaling NAT and Media NAT in the Ingress and Egress Trunk Groups. 3. Make an Audio and Video call between the NATed EndPoints EP1 and EP2. 4. After a call gets established, the EP1 and EP2 sends Audio and Video packets. 5. NAT learning happens for Audio and Video and then the packets are sent and received from EP1 and EP2.	The code is modified to process the NAT learning for the video stream in the D-SBC. **Workaround:** None.
SBX-103353	2	The AddressSanitizer: detected heap-use-after-free /localstore/ws/jenkinsbuild/sbxmainasan/marlin/SIPSG /sipsgCallNotification.c:1123 in SipSgSendCallNotificationApi(SIPSG_CCB_STR*, SIPSG_CALL_NOTIFY_TYPE_ENUM, sip_nameaddr_str*). **Impact:** While freeing up a SIP call, the code is accessing the SIP call control memory block immediately after it has been freed up in the same processing loop. **Root Cause:** This issue was detected using ASAN images, it has not been proven to cause bad behaviour using regular production images, but accessing memory after it has been freed can cause unexpected processing to happen which might potentially result in coredumps. **Steps to Replicate:** Run regular call scenarios with ASAN images.	The code is modified to avoid using the memory block after it is free. **Workaround:** None.

SBX-104016	2	Anomalies were observed after decoding a ACT File by sbxCamDecoder.pl. **Impact:** Issue 1: The camDecoder script "sbxCamDecoder.pl" does not decode a reboot, the switchover records. Issue 2: It does not display the field names under the "Ingress Signaling Information" and "Egress Signaling Information" for an EVENT records as shown below. 26. Ingress Signaling Information : 26.1 : "sip:7587339665@10.xx.xxx.xxx 26.2 : 1-23946@10.xx.xx.xxx 26.3 : <sip:sipp@10.xx.xx.xxx:xxxx>;tag=23946SIPpTag011 26.4 : <sip:7587339665@10.xx.xxx.xxx> 26.5 : 26.6 : sip:sipp@10.xx.xx.xxx:xxxx 26.7 : 26.8 : 26.9 : 26.10 : 0 26.11 : 26.12 : 26.13 : 26.14 : 1 26.15 : 26.16 : 26.17 : 26.18 : 26.19 : 26.20 : 26.21 : 26.22 : 26.23 : 26.24 : 26.25 : " **Root Cause:** The sbxCamDecoder script was not updated to support the reboot, on switchover records. Also, the script was not updated to decode "Ingress Signaling Information" and "Egress Signaling Information" for EVENT records. **Steps to Replicate:** Issue 1: The switchover record issue. Setup: The SBC HA Procedure: 1. Perform a switchover the SBC. 2. Decode the latest ACT log that contains "SWITCHOVER" record by using the sbcCamDecoder.pl. Issue 2: REBOOT Record issue. 1. Reboot the SBC. 2. Decode the latest ACT log that contains the "REBOOT" record, by using sbcCamDecoder.pl. Issue 3: 1. Send an OOD message (OPTIONS). 2. Decode the latest ACT log that has the event RECORD by using the sbxCamDecoder.pl.	sbxCamDecoder was updated to support decoding REBOOT, SWITCHOVER records and the "Ingress Signaling Information" and "Egress Signaling Information" in the EVENT Records. **Workaround:** Decode the record manually.
SBX-103894	2	The AddressSanitizer: detected heap-use-after-free on address 0x61b000018f84 at pc 0x556c7afd4213 bp 0x7fcbf0905680 sp 0x7fcbf0905678. **Impact:** An invalid memory access of a termination object after it's been deleted. Accessing the memory after it has been freed can result in unexpected behaviour and in the worst case coredumps. **Root Cause:** In the call teardown processing, after the last termination is deleted, the calltracing function was accessing the already deleted call termination object to retrieve the context ID. **Steps to Replicate:** 1. Setup a call in MRFP. 2. Teardown the call. 3. The previously mentioned invalid memory access occurs in handling the deletion of the last termination of the call.	In the same function, retrieve the context ID from the context object instead to address the issue. **Workaround:** None.

SBX-103814	2	The RECORDING CDR does not have correct value for the SRTP field during switchover scenario. **Impact:** For the SIPREC sessions with SRTP, after a switchover the "RECORDING" CDR generated had values as 0 in the SRTP statistics fields as shown below: 24.7 ingress SRTP info1 : 0:0:0:0 24.12 egress SRTP info1 : 0:0:0:0 **Root Cause:** The standby processing code did not support copying the SRTP information into the SIPREC Standby data blocks and as a result was lost during a switch over. **Steps to Replicate:** 1. Execute a SIPREC call, with a SIPREC Session over the SRTP. 2. Perform a switchover. 3. Verify the RECORDING CDR for SRTP Statistics in the following fields: 24.7 ingress SRTP info1 : 0:0:0:0 24.12 egress SRTP info1 : 0:0:0:0	The code is modified to process the SIPREC SRTP information is added. **Workaround:** None.
SBX-103807	2	The SBC disables the SRTP for an audio when the EP disables and re-enables the audio. **Impact:** The SBC disables the SRTP for audio when EP disables and re-enables the audio. **Root Cause:** During the modify offer processing, the SRTP value is taken from previous Active security PSP without checking if the SRTP is valid or not. **Steps to Replicate:** Test Procedure: Setup Audio+Video RTP to SRTP pass-Thru call between UAC-UAS: 1. UAC sends invite with Audio and video. 2. UAS responds with Audio and Video cryptoline. 3. UAC sends re-invite to disable Audio stream port=0 and inactive and Video with valid media port and sendrecv. 4. UAS responds 200OK with port=0, a=inactive and no crypto line for audio and video with valid port and crypto line. 5. UAC sends re-invite to add Audio stream back with valid media port and sendrecv and video with valid media port and sendrecv. 6. UAS responds 200OK with valid Audio and Video crypto lines. Expected Result: 1. RTP-SRTP A+V call gets established. 2. The SBC disables audio stream and sets up RTP-SRTP call with video stream. 3. The SBC re-establishes Audio+Video RTP-SRTP call. Actual Result: 1. RTP-SRTP A+V call gets established. 2. The SBC disables audio stream and sets up RTP-SRTP call with video stream. 3. The SBC re-establishes re-Invite without SRTP for audio stream.	The code is modified to copy the Active security PSP only if the SRTP admin state is enabled. **Workaround:** None.
SBX-105310	2	There was a SM Process leak for the MRFP call on the MRFP active. **Impact:** The redundancy group manager (RGM) that is used in conjunction with N:1 deployments has a memory leak. **Root Cause:** The RGM handles the switchover and fault messages in N:1 deployments and it was not freeing up the ICM message after processing that results in a memory leak. **Steps to Replicate:** This issue was observed in an MRFP configuration especially when restarted instances.	The code is modified to correctly free the ICM messages. **Workaround:** None

SBX-103603	2	The LeakSanitizer: detected memory leaks in the MrfRmProcessTrmAllocRpyMsg. **Impact:** While testing call scenarios for RTCP for T.140 Pass-through functionality, it was observed that the SCM process could leak memory for calls associated with an MRF (external media transcoder). **Root Cause:** The SBC was allocated memory while processing the SDP associated with this call but was not always freeing up the memory at the end of the call. **Steps to Replicate:** Run various call scenarios with MRF where the SBC is using the SIP to allocated media resources on an external media transcoder (MRF) or T-SBC.	The code is modified to correctly free all the memory allocated for the call. **Workaround:** None.
SBX-103731	2	The AddressSanitizer: detected heap-buffer-overflow on address 0x61a0000cb9d9 observed in the SAM Process while running OCSP feature. **Impact:** When the OCSP stapling feature is enabled on the SBC and the code was processing the response it writes to unallocated memory and in the worst case this could result in process coredumps. **Root Cause:** While processing OCSP response the code was allocating a memory buffer large enough to hold the response, but then incorrectly writing one byte off the end of the memory buffer while attempt to try and null terminate the string. **Steps to Replicate:** Setup - **UAC** > **Dut**<>**Adapter** -> **UAS** 1. Create an OCSP profile by configuring the defaultResponder and stapling enabled. 2. Attach the OCSP profile to the TLS profile configured. 3. From Endpoint A, Intiate the TLS call with Client Hello from the SIPP UAC having OCSP parameter in it. 4. The SBC should send server hello certifciate to the user client.	The code is modified to correctly terminate the OCSP response string without writing off the end of the memory buffer allocated to hold the response. **Workaround:** None.
SBX-103801	2	Observed the run time error in M-SBC "runtime error: load of value 42, which is not a valid value for type 'bool'" **Impact:** The M-SBC could potentially configure the wrong data path mode for a call. **Root Cause:** No issues were observed while running this functionality on a regular deployment image. But while testing with ASAN, it highlighted that some of the fields used in a call resource allocation message were not always initialized correctly, which could potentially lead to unexpected behaviour e.g. SYS_ERRs, wrong datapath mode setup. **Steps to Replicate:** This issue was highlighted while while running test suite related to RFC-4117 MRF Mid-Call modification Enhancement	The code is modified to correctly initialize the resource allocation request fields to avoid issues. **Workaround:** None.
SBX-98024	2	The contact header is not transparently passed when the Ingress and Egress had different transport types. **Impact:** Contact header is not passed transparently from Ingress, when egress side has different transport type, even when the IPSP flag 'passCompleteContactHeader' is enabled on both ingress/egress Trunk Groups. **Root Cause:** In API SipSgCheckAndSetContactHeaderTrasparency(), irrespective of transparency control is enabled/disabled, if the egress Sig Zone is MS Teams, then contact header was not transparently passed to egress. **Steps to Replicate:** 1. Configure, IPSP flag 'passCompleteContactHeader to enable. 2. Attach the IPSP to both ingress/egress TG's. 3. Set Ingress transport to TCP / Egress to TL. 4. Create pathCheck profile with hostName 'sip.pstnhub.microsoft.com' and attach to the Teams side. 5. Make a successful call.	The code is modified so regardless of MS Teams zone, if the transparency control flag is enabled then pass the contact header transparently to the egress. **Workaround:** None.
SBX-101937	2	The one medium vulnerability found after the Qualys Scan. **Impact:** A medium vulnerability found after the Qualys Scan in Jquery 3.4.1 version. **Root Cause:** The jquery 3.4.1 version has security issue. **Steps to Replicate:** Run a Qualys Scan and vulnerability was not shown.	The code is modified to address the issue. **Workaround:** No workaround.

SBX-102718	2	The Confd updateAdmin user's configuration was failing. **Impact:** In cloud deployments, when a new user is created, it throws the error: "Cannot change accountAgingState to disabled while accountRemovalState is enabled" even though accountAgingState is set from disabled and accountRemovalState to disabled. **Root Cause:** The validation logic for user creation was done along with transformation callbacks. This makes the validation logic to be order dependent. **Steps to Replicate:** 1. Launch a cloud standalone instance. 2. Create a new user with accountAgingState to disabled and accountRemovalState to disabled: commit fails with error "Cannot change accountAgingState to disabled while accountRemovalState is enabled"	The code is modified to make an order independent. **Workaround:** None.
SBX-103634	2	The LeakSanitizer: detected memory leaks in DCmRestoreAllMetaVarsToStandbyContext. **Impact:** A small memory leak was observed in the SAM process while performing a switchover from standby to active box. **Root Cause:** The standby instance stores information about the metavars associated with signaling ports configured on the active instance. During the conversion from standby to active, the standby data is moved into active structures but the original standby memory blocks are not freed up correctly resulting in a memory leak. **Steps to Replicate:** Perform a switchover from standby to active while running a basic call, no memory leak will be observed in the SAM process.	The code is modified to correctly free the memory associated with the standby data when it gets transitioned to active to avoid the memory leak. **Workaround:** None.
SBX-104360	2	The SWITCHOVER ACT Records are not generated in the SBC with HA mode set as Nto1. **Impact:** On an N to 1 system, the SWITCHOVER record is not written to the accounting file on the new active node after a switchover. **Root Cause:** The SWITCHOVER record is sent to the ENM process before it has opened the accounting file, so the record is not written. **Steps to Replicate:** 1. Perform a switchover a system. 2. Check that the switchover record is written to the accounting file.	The SWITCHOVER record is stored and then written out when the accounting file is opened to address the issue. **Workaround:** None.
SBX-104826	2	The SBC fails to relay to 3xx and picks the next route when Ethe nhancedLocalRedirection and StatusCode3xx flags are enabled. **Impact:** The SBC fails to relay the received 3xx to the ingress side and picks the next route when the EnhancedLocalRedirection and StatusCode3xx flags are enabled with 2 routes. **Root Cause:** When both the StatusCode3xx and EnhancedLocalRedirection are enabled for the 2 routes scenario, the performCrankback is set to true which leads to this issue. **Steps to Replicate:** Procedure: 1. Configure the SBC for A to B call over ERE. 2. Configure the ERE to return two routes for Initial call R1, R2. 3. Enable the flag statusCode3xx, EnhancedLocalRedirection on TG IPSP. 4. Send the INVITE from UAC. 5. Send the 300 Multiple Choice from UAS with Contact header and embedded headers.	The code is modified to ensure that performCrankback is not set to true when both the EnhancedLocalRedirection and StatusCode3xx are enabled. **Workaround:** None.

SBX-91592	2	The DRBD tuning is not optimal. **Impact:** On the non-cloud 1:1 SBCs, due to non-optimal tuning of the DRBD, the DRBD connection between active was getting disconnected leading to full sync and high i/o on the DRBD partition. **Root Cause:** Due to the peer not responding within a certain time (ko-count * timeout), ko-count feature of DRBD was disconnecting the peer leading to full sync. **Steps to Replicate:** The following are the steps to test the changes: 1. Decrease the timeout value in the DRBD conf file. 2. Restart the DRBD service. 3. Resume the DRBD sync if not already enabled. 4. Check syslog, the DRBD must not get disconnection logs.	The DRBD ko-count feature is disabled on the SBC to address the issue. **Workaround:** None.
SBX-101743	2	The SBC start is showing some errors related to a serf file and config-version file. **Impact:** Missing the file error printed to terminal. **Root Cause:** The gluster setup script does not redirect output of 'cat' command. **Steps to Replicate:** Run the sbxstop; sbxstart	The 'cat' command error output is redirected to NULL to fix the issue. **Workaround:** None.
SBX-91799	2	The segfault in pamValidator during PM login with incorrect credentials. **Impact:** The segfault in pamValidator on a failed login for locked user. **Root Cause:** The pamValidator defines a conversation function that is called by pam modules to exchange values. The pam module was freeing a struct member in the first call and accessing the same freed value in another call to the conversation function that was causing segmentation fault. **Steps to Replicate:** Perform following steps on any of the SBC deployment and verify that segmentation fault does not happen: ## TEST 1: Ensure success for correct username and password: 1. Encode username and password to base 64 and set as environment variables USER and PSWD example: export USER="YWRtaW4=" ; export PSWD="U29udXNAMTIz" 2. Run pamValidator and verify it returns success. ##TEST 2: Authentication Failure for username and incorrect password: 1. Encode the correct username and incorrect password to base64 and export as env variables USER and PSWD. 2. Run pamValidator and verify it returns "Authentication Failure". 3. Run pamValidator again multiple times (atleast 3 more) and verify the authentication failure and no segmentation fault. 4. Wait for 30 seconds and try TEST#1 with the correct password and verify it succeeds.	The code is modified so the pam_response struct properly in between calls to the conversation function. **Workaround:** None.

SBX-105152	2	While expecting a 200 OK to ingress endpoint, the SBC was sending BYE to the Egress endpoint. **Impact:** If the Media inactivity/activity monitoring is enabled on media leg, and if media is not received at all on that leg in initial 10 seconds, then the NP sends a media inactive notification to up layer. But later even if media starts coming to the SBC on that leg, the NP is not sending media is active now in notification to Application layer. As a result, the application layers were closing the call based on the action configured for media inactivity (peerAbsenceTrapAndDisconnect). **Root Cause:** In the call, if the media is preceded by no media for few seconds. The call can be terminated if the peerAbsenceAction is peerAbsenceTrapAndDisconnect. **Steps to Replicate:** 1. Configure the peerAbsenceAction as peerAbsenceTrapAndDisconnect in the PSP. 2. After the call is established, do not stream the media for initial few seconds (this duration should be less than inactivityTimeout), start it only after few seconds. > set system media mediaPeerInactivity inactivityTimeout 20 > set profiles media packetServiceProfile DEFAULT peerAbsenceAction peerAbsenceTrapAndDisconnect 3. In this case, the pause should be less than 20 seconds. 4. With the fix, the calls will not be terminated.	The code is modified to fix the Inactive to Active detection functionality and address the issue. **Workaround:** If media is expected to come late, they should not configure the peerAbsenceAction action in PSP to peerAbsenceTrapAndDisconnect. The action can be selected as the peerAbsenceTrap or none.
SBX-105679	2	The ASAN leaksanitizer detected errors in the CPX and SCM. **Impact:** The SCM and CPX processes have a small memory leak while changing the IPsec and IP interface group configuration. **Root Cause:** While processing configuration related commands, the SBC was reading information from CDB into temporary memory blocks but failed to release the memory at the end of the configuration action, resulting in a small memory leak. **Steps to Replicate:** Make the configuration changes to IPsec and IP interface group.	The code is modified to ensure the memory is correctly freed up to avoid the leak. **Workaround:** None.
SBX-105637	2	The AddressSanitizer: detected heap-buffer-overflow on address 0x61b000013128 at pc 0x55e3eea0419e bp 0x7ff7a52768a0 sp 0x7ff7a5276898 in ScmProcess_0. **Impact:** There was invalid memory access when the SBC receives the 500 Internal Error to REGISTER. **Root Cause:** The root cause of this issue is accessing invalid memory while accessing callData, trying to read off the data from the end of memory block. It can potentially cause the coredumps if the memory block is at the edge of the accessible memory region. **Steps to Replicate:** Testcase: Description: 1. Clean up SAs if unexpected response received Procedure: 1. Monitor the exchange. 2. Send an initial reg message. 3. Receive the 401 challenge. 4. S-CSCF responses with 500. Expected Results: 1. Verify IPsec SA's deleted (ip xfrm state).	The code is modified to access the respective application data (It can be call data, registration data or subscription data) based on type of SIP message. **Workaround:** None.

SBX-104990	2	In a secure call, the SBC does not increment the port number in R-URI after processing Refer. **Impact:** In a secure call with TLS configured, if the call is REFERed with a REFER-TO header containing a FQDN and port number, the SBC sends out a new INVITE to specified FQDN and port number. If that INVITE fails and the SBC then sends a subsequent INVITE on the next route, it does not correctly increment the RURI port number for the TLS. **Root Cause:** The SBC code does not take into account that a re-route after a REFER-TO with FQDN and port number target needs to increment the port number for TLS, if the target after the re-route is different to the original target specified in the REFER-TO. **Steps to Replicate:** 1. With the recommended SBC configuration for MS Teams with TLS enabled between the SBC and MS Teams, establish a call from the PSTN to MS Teams 2. Send a REFER from MS Teams that includes following header: REFER-TO: <sip:sip2.pstnhub.microsoft.com:xxxx;transport=tls> 3. Based on the REFER, the SBC should route the call and send an INVITE to sip2.pstnhub.microsoft.com using port xxxx 4. Reject this INVITE from MS Teams with a 503. 5. The SBC should then send an INVITE out using the second route to sip3.pstnhub.microsoft.com using port xxxx. 6. Complete the call signaling and verify referred call is established correctly.	The code is modified to increment the RURI port number for TLS if performing a re-route to a target FQDN and port number that is different to the original target specified in the REFER-TO. **Workaround:** None.
SBX-104671	2	The CpxAppProc leak for the MRFP call. **Impact:** During the SBC startup, the CPX process has a small memory leak. **Root Cause:** During the SBC startup processing, the CPX process reads various CDB configuration and performs DB schema upgrade validation logic. As part of this processing, it was creating temporary internal memory blocks but not releasing them at the end of initialization. **Steps to Replicate:** Restart the SBC after it has been configured.	The code is modified to correctly release the temporary memory blocks used for initialization processing. **Workaround:** None.
SBX-105339	2	The LeakSanitizer: detected memory leaks on the active OAM. **Impact:** The CPX process was leaking small amounts of memory while processing BFD configuration changes. **Root Cause:** The CPX process was allocating memory in order to interact with the CDB while process BFD configuration changes. But it was not freeing up the memory at the end of the configuration action, resulting in a memory leak. **Steps to Replicate:** Make configuration changes to the BFD profile.	The code is modified to correctly free the memory required to process the BFD configuration changes and avoid the memory leak. **Workaround:** None.
SBX-105262	2	The SBC is sending an unexpected re-INVITE to the Egress side in the SRTP early media scenario. **Impact:** The SBC is sending an unexpected re-INVITE to the Egress side in the SRTP early media scenario. **Root Cause:** This issue is caused as a side-effect of SBX-103807. **Steps to Replicate:** Run the following call flow: 1. The UAC sends an INVITE with 100 rel required. 2. The UAS sends 18x with SDP and SRTP(SHA-1-32). 3. Ingress sends PRACK with SDP and SRTP(SHA-1-32).	Copy an active security PSP only if audio stream is present to address the issue. **Workaround:** None.
SBX-104537	2	Observed SIPFE MAJOR logs on the n1-standard-4 SBC_HA_HFE_SPLIT instance. **Impact:** The log was printed as major, when stale calls are present and whenever we start cleaning the stale calls, then the log is seen. **Root Cause:** This log is expected when clearing any stale calls. **Steps to Replicate:** Run call load and if any stale calls are seen, then this log issue is seen (only when the Minor logging is enabled).	The code is modified to address the issue. **Workaround:** None.

SBX-103851	2	Observed an error "runtime error: index -20 out of bounds for type 'uint8_t [16]' " on UXPAD when running T140 call with out-of-order of T.140 packets. **Impact:** If the T140 packet contains any T140block that has more than 16 characters, then a debug buffer to display the ASCII characters of T140 packet may write beyond its size. **Root Cause:** The debug buffer to display ASCII characters of T140 packet is 16 bytes in size. It saves the 16 bytes of last T140block. However, the T140 packet SBC accepts allows a maximum T140block size of 36 characters. The code did not properly limit the size of buffer to copy to 16 characters. **Steps to Replicate:** 1. Make a SIPP call (AMRNB=>G711) with t140=>baudot enabled. 2. Send PCAP with the T140 from AMRNB termination having T140block in packet exceeding 16 bytes. 3. There may not be any observable effect, but the debug buffer that displays ASCII characters writes beyond its bounds and corrupts some other fields in the structure.	The code is modified to limit the size of ASCII buffer to copy to 16 characters. **Workaround:** None.
SBX-105270	2	There was a CpxAppProc leak for MRFP calls. **Impact:** The small memory leak occurs on the SBC/MRFP nodes when action/status/stats under the node branch is accessed through the OAM node CLI or EMS. **Root Cause:** Resource references are cleared mistakenly after serving the request from the OAM node. **Steps to Replicate:** Execute a node branch command repeatedly and monitor the CPX process size on the target node.	The resource references are cleared only when the system is shutting down. The resources are now getting reused by subsequent requests to address the issue. **Workaround:** Avoid using the node branch commands in automated /periodic operations. Manual use should work as the leak is small.
SBX-105114	2	The usage of a kill command output in the active and standby CE_node logs. **Impact:** The kill command usage gets printed in the CE_Node log file of the managed nodes. **Root Cause:** No glusterfs process is present when the kill command is executed by the glusterSetup.sh script called by sbxConfigUpdater.sh. **Steps to Replicate:** 1. Reboot the Standby OAM. 2. Ensure that kill usage does not appear in the CE_Node log file of the managed nodes.	Redirect the kill command error output to /dev/null to address the issue. **Workaround:** None.
SBX-105395	2	There are coverity issues in the OAMNODE. **Impact:** When processing a show list command under the node branch from the OAM node, if the target node fails to read the command path in the request, the code will access memory immediately after freeing it. While in most cases this should not cause issues, accessing memory after it is freed is not good behaviour and could result in unexpected behaviour, potentially causing coredumps. **Root Cause:** The error handling flow in the code is incorrect. The handling code hits some code for the success flow. **Steps to Replicate:** Enter the CLI commands like "show table/status node SSBC-1 <path to some list> <partial key>" and hit "tab" for auto completion on a system with an unreliable HA network. Repeat until the target node showing this error in its DBG log: CPX ConfdProxy::worker: could not deserialize parameter for PROXY_FIND_NEXT_REQ	The code is modified to address the issue. **Workaround:** None.
SBX-103103	2	The BFD packet forwarded by the router is not received by the MRFP. **Impact:** Once the BFD session is established on a port (either primary or secondary), an immediate port switch over is followed due to the BFD packets dropped at NP for a brief amount of time (~1 second). This eventually triggers a node switchover. **Root Cause:** A race condition in ACL lookup is the cause of this issue. **Steps to Replicate:** 1. Ensure the BFD session is up on a port (either primary or secondary). 2. Initiate a port switchover. 3. Monitor if the BFD session comes back on the switched-over port and an immediate port switch over is not followed.	The code is modified to address the issue. **Workaround:** A user ACL can be added as a workaround.

SBX-103984	2	For an existing call trace, when the call trace feature is disabled on the MRFP, the MRFP should reject the trace request (in MODIFY with CALLTRACE/TRACEACTIVITYREQUEST=ON) from the C3 by sending a NOTIFY to the C3 with RES=FAILURE. **Impact:** When the call trace feature is disabled in the MRFP (using CLI command: set global callTrace state disabled), and the C3 tries to enable call trace using the MODIFY command with CALLTRACE /TRACEACTIVITYREQUEST=ON, then the MRFP should reject the trace request from C3 by sending NOTIFY to C3 with {CALLTRACE/TRACACT {Stream=1,RES=FAILURE}}. However, the MRFP (9.1 R0) is not sending any NOTIFY message for the Call Trace request received in the MODIFY command. **Root Cause:** The issue was seen only when the MODIFY command does not have any SDP. **Steps to Replicate:** 1. Disable the call trace feature, using the CLI command: set global callTrace state disabled. 2. Establish a MRFP call for the SBC from C3 by sending two ADD termination commands. 3. Send MOD termination command from C3 with: CALLTRACE /TRACEACTIVITYREQUEST=ON.termId ip/1/intf/3523215361{ Media { Stream = 1 { LocalControl { Mode=SendReceive, CALLTRACE/TRACEACTIVITYREQUEST=ON } } } ,Events = 1 { NT /NETFAIL , ADID/IPSTOP { DT=50 } , HANGTERM/THB { TIMERX=1800 } } ,Signals { } } 4. Since call trace is disabled at the SBC, verify that the SBC sends a NOTIFY with res=Failure after sending a MODIFY reply.	The code is modified to send a NOTIFY for TRACEACTIVITYREQUEST when the MODIFY command does not result into any change in media parameters. The MRFP now sends a NOTIFY with RES=SUCCESS /FAILURE (based on call trace configuration) after sending reply for the MODIFY command. **Workaround:** None.
SBX-104325	2	A SCM core dump was observed when multiple gateway TGs are created in a GW-GW call on a HA setup. **Impact:** On a HA setup, the Standby box SCM Process dumps core when the Standby starts to sync from Active post a switch over and as a result, the switchover occurs after a scenario where Gateway TG's are created and then a GW TG with a lower index (created earlier) is deleted. Example: 1. Create GWTG1, GWTG2 and GWTG3. 2. Delete GWTG2 3. Switch over. **Root Cause:** The coredump is caused due to difference in indexing the gateway TG's in active and standby boxes. The GW TG indexes were out of sync between the Active and Standby. Active SBC had holes in the indices of the GW TGs after deletion. The Standby SBC does not have holes for the GW TGs that are present post deletion and occupy a different index when compared to active. **Steps to Replicate:** 1. The HA setup with GW-GW configurations. 2. Create 3 Gateway Trunkgroups: GWTG1, GWTG2 and GWTG3. 3. Delete the GWTG2. 4. Perform a switchover.	The code is modified to ensure that the GWTG indexes on the Active and Standby are in sync. **Workaround:** None,
SBX-104693	2	When multiple codecs are received in descriptor, the call is getting rejected if license of the first preferred codec is not present in the license bundle. **Impact:** When the MRFP receives an ADD termination command with a list of codecs in the audio stream from the MGC, it rejects call if the license of first preferred codec is not present in the license bundle, even though MRFP could have succeeded the call with other codecs on the list. **Root Cause:** The MRFP's codec filtering function chooses the first allowed codec from the list and send it to media plane without check the codec license, so that the media plane returns error in case of codec license validation failure. The call failed as a result. **Steps to Replicate:** 1. Ensure the MRFP is up and running 2. Generate a license xml with ONE unit of MRFP-RTU, MRFP-DSP-RTU MRFP-DSP-AMR and ZERO units MRFP-DSP-AMRWB. Install the license bundle b1 in MRFP. 3. Place a call from endpoint with AMRWB and AMRNB in SDP in same m line 4. Validate the call should be succeeded with AMRNB codec being used.	The code is modified so it always chooses a codec with a valid license to the media plane. **Workaround:** None.

SBX-103281	2	The route data was lost after offline PM upgrade from 625R0 to 823A13. **Impact:** The special character data (e.g. ?,*,#,$) is not getting migrated from the Oracle version to postgres version. **Root Cause:** Special characters were causing issues with Postgres data loading. **Steps to Replicate:** 1. Create 100+ routes that have special characters in the DN field (Domain Name) in the SBC 6.2.5.R0. 2. Upgrade to the SBC through the PM offline upgrade to 8.0 or above. 3. After upgrade all route data was lost while other data are unaltered.	The code is modified to address the issue. **Workaround:** No workaround.
SBX-102445	2	The media port range threshold alarm is not triggered after a switchover. **Impact:** The sonusMrfpRealmMediaPortRangeThresholdExceededNotfication alarm does not get raised on a newly active box following a switchover, even if the conditions for the alarm are met. **Root Cause:** The realm status is not getting properly mirrored to the standby box. **Steps to Replicate:** 1. Run calls such that 90% of the ports are used and alarm is triggered. 2. Trigger a switchover from the active MRFP. 3. Alarm should be triggered in new active MRFP.	1. The code is modified to check the UDP port usage, and to raise the alarm if appropriate. 2. The code is modified to mirror realm status so that, it can be used to raise alarm when transitioning to active or when new call on SBY arrives. **Workaround:** None.
SBX-104963	2	The createConfigDrive.py --file option throws an error when executing. **Impact:** In the case of KVM/VMware deployments with qcow2/OVA/vmdk, the createCOnfigDrive.py script that creates the config-drive is not working with the '--file' option. **Root Cause:** There was an error in handling the '--file' option **Steps to Replicate:** Generate a configuration drive with the '--file' option.	The code is modified to address the issue. **Workaround:** Use the '--cli' option to generate a configuration drive.
SBX-103761	2	The createConfigDrive.py --cli throws an IndentationError. **Impact:** When deploying on the KVM/VMware using qcow2/OVA/VMDK and generating config-drive using createConfigDrive.py with '--cli' option, the script returns with an error. **Root Cause:** There was an indentation issue in the Python code. **Steps to Replicate:** Generate a config-drive with the '--cli' option and verified the generated config-drive.	The code is modified to address the issue. **Workaround:** None.
SBX-103682	2	The LeakSanitizer: detected memory leaks at confd_malloc **Impact:** The ASAN detected memory leaks while processing the E164 profile configuration changes. **Root Cause:** The code was allocating memory while processing E164Profile configuration changes but not releasing the memory at the end of the configuration action, resulting in a small memory leak. **Steps to Replicate:** Create and modify the E164Profile configuration.	The code is modified to release the internal memory block at the end of the configuration action. **Workaround:** None.
SBX-103821	2	The AddressSanitizer: detected heap-use-after-free on address 0x6180000ed180 at pc 0x5619a742719d bp 0x7f3b04960310 sp 0x7f3b04960308. **Impact:** While the MRFP node is shutting down, it can access memory after it has been freed, this could result in unexpected behaviour and in the worst case a coredump. But would have limited impact as it only occurs when shutting down. **Root Cause:** During the sbxstop/sbxrestart or switchover because of race-condition, when the SBC is in deactivation the oamNodeRegisterRetry can access already deallocated resource leading to a core dump. **Steps to Replicate:** 1. Setup a build with HA MRFP using OAM. 2. Do the sbxrestart/switchover of an active instance.	The code is modified to handle this race condition. **Workaround:** None.

SBX-105312	2	The trunkgroups are not displayed while assigning the SMM profile to TG on the EMA. **Impact:** The trunkgroups are not displayed while assigning the SMM profile to TG on the EMA. **Root Cause:** The dropdown height is limited, and as the result the last entry is not visible. **Steps to Replicate:** 1. Create more than one TG. 2. Create a SMM profile on EMA. 3. Click on Assign SIP Adaptor Profile. 4. Under 'Assign Message Manipulation Profile to TGs', check for Input Adaptor and Output Adaptor. All the options should be available after performing the test steps.	The code is modified to show all the options to select. **Workaround:** None.
SBX-98283	2	The SBC is unable to find the TG for in-dialog NOTIFY message when received from different IPs and the dialogTransparency flag. **Impact:** When the indialog NOTIFY comes from different source IP, then the SBC is dropping the NOTIFY. **Root Cause:** The existing design for OOD does not support the indialog NOTIFYs when it comes from a different source. **Steps to Replicate:** 1. Initiate a SUBSCRIBE dialog. 2. Send an indialog NOTIFY from a different source.	The code is modified to accept the indialog requests when the source is different. **Workaround:** None.

Known Issues

Known Issues in Release 09.02.01R001 to 09.02.03R002

The following known issues exist in these releases.

Table 36: Known Issues

Issue ID	Sev	Problem Description	Impact/Workaround
SBX-113524	3	The SBC is not forwarding the received 200 OK message and fails the call.	**Impact Statement:** When using a GW-GW for direct media calls between signaling only SBCs, the 200 OK message is not being passed along and the call fails. **Workaround**: Disable the following control: set global signaling sigOnlyMode sigOnlyModeValue
SBX-99023	2	The CE_2N_Comp_Sm Process is dumping core.	**Impact Statement:** The SBC coredump directory shows a SM Process coredump, but services are not affected and they keep running. **Workaround:** You can remove the coredump from the SBC coredump directory. No other action is required since these types of cores do not cause the SBC services to go down.
SBX-111973	2	On a LRBT with lateCrankback, the call is torn down upon Hold.	**Impact Statement:** If a call route advances after lateCrankback and LRBT is enabled, the call is torn down upon egress connect (200 OK) after hold/resume request. **Workaround:** None.
SBX-111461	2	The SBC plays a LRBT using PCMU when the negotiation happened with AMRWB in the LM call.	**Impact Statement:** The tone played is with an old negotiated codec instead of codec selected by ingress endpoint in Prack. Issue is seen only when multiple codecs are sent in late media offer in 180 with sendSbcSupportedCodecsForLateMediaReinvite flag enabled. **Workaround:** None.
SBX-111460	2	The SBC does not offer the 16K dtmf in a LM call when the SDP is present in 2xx.	**Impact Statement:** The SBC is not sending 16k 2833 Payload type in the initial offer towards the ingress when the SDP is present in 2xx during a Late media "convert" call. **Workaround:** None.
SBX-111351	2	The CHM process is coring after recovering from a splitbrain.	**Impact Statement:** While successfully recovering from a split-brain in a specific scenario, it is sometimes noticed that a CHM coredump is created. **Workaround:** None. The system does recover correctly without any manual intervention.
SBX-110134	3	For a T140 call - one-way audio observed if NAPT enabled on egress.	**Impact Statement:** If NAPT for media is enabled, the dest media port (NAPT media) stays set to 0. **Workaround:** None.
SBX-111034	2	Unable to login as an admin user using keys after cleanDB.	**Impact Statement:** User is unable to log in to the Confd CLI using 'admin' user private SSH key after running clearDBs.sh script. **Workaround:** Do not run the clearDBs.sh script.
SBX-103724	2	The RECORDING CDR does not have Media data and stats field in a REFER scenario case.	**Impact Statement:** The Media Stats are not present in the Recording CDR when we record the C Leg. **Workaround:** None.
SBX-101226	2	The OAM should not configure the same IP and port for two different VMGs.	**Impact Statement:** The mis-configuration that was using the same IpVar for two different VMGs does not throw an error in the OAM CLI. **Workaround:** None. The mis-configuration recovery requires a reboot.

SBX-105824	2	The glusterfs had a core dump on the Active OAM for the T-SBC post upgrade.	**Impact Statement:** The OAM node is using the third party package glusterfs and we are using version 3.8.8-1. During a scenario where both OAM nodes are starting up, we may encounter an intermittent core from the glusterfs process. The OAM functionality is not impacted by this core and it does not impact the shared directory that is mounted by the gluster process. The call processing nodes that are managed by the OAM are not impacted and their configurations are unaffected. **Workaround:** No workaround. The core maybe be produced during simultaneous reboot of OAM nodes but the functionality of the OAM nodes is not impacted.
SBX-105921	3	Reduced the configuration limits that need to be used for certain fields.	**Impact Statement:** The CDB schema supports larger strings than the SBC application code can currently support for the following configuration objects. This issue is due to the SBC application code not allowing for one additional character to include the string null terminator if the configuration in CDB actually contains the maximum number of characters. The maximum size the application can be supported, even though CDB schema would allow for one character more to be entered. addressContext/diamNode/realmRoute/realm - 128 characters global/genericCodec/audioEntry/name - 49 characters system/policyServer/remoteServer/fqdn - 255 characters global/signaling/srvcc/stnSr - 30 characters global/signaling/srvcc/eStnSr - 30 characters global/signaling/srvcc/pstopSti - 30 characters profiles/services/testCallNumberProfile/testCallNumber/number - 23 characters In a future release, the application code will either be extended to allow for one more character or validated to put in place to restrict the character size to one less. **Workaround:** Use the reduced size for the fields as mentioned in the Impact Statement.

Known Limitations

The following limitations exist in this release:

1. The Access Control List (ACL) is not installed to configure SNMP traps for accepting traffic. A dynamic ACL is added to configure SNMP traps. An ACL must be installed for SNMP traps for accepting traffic.
2. The physical NIC connectivity must be in active state at the hypervisor level before starting the SWe instance on the SBC SWe platforms. In case of SWe instance with SR-IOV interfaces, manual restart of the SWe instance is required if physical NIC connectivity goes down while the instance is in progress.
3. The Antitrombone feature is not supported on the D-SBC.
4. EMS identifies the nodes based on the VNFC-ID. While instantiating SBC/PSX cloud nodes, ensure that you use a unique VNFC-ID only. If you reuse an existing VNFC-ID, EMS treats this as a re-registration request and overwrites the existing data on the cloud node.
5. While configuring the SBC SWe Cloud instances, the CLIs commits successfully even if any metaVariable provided is incorrect. The SBC SWe Cloud instance cannot validate the CLIs, as the CDB configuration file is stored in the OAM Node and is shared among all the other SBC SWe Cloud instances in the cluster.
6. Editing IP Interface is not reflected in the if configuration (ifConfig). This behavior is observed only on the S-SBC when action is set to "dryup" mode on the IP Interface. The IP address changes are not updated in the kernel and will not be displayed when ifconfig linux command is executed. In case of S-SBC, if the ipInterface configuration needs to be modified and if the action is set to "dryup" in ipInterface configuration, it must be set to "force" before disabling the ipInterface and making any changes.
7. A LSWU on an SBC 7000 should only be performed when the total number of active calls on the system is below 18,000. If the criteria is not met, a double failure during the upgrade may occur thereby losing all active calls. If such a failure occurs, both active and standby SBC services will go down. Contact Ribbon Support immediately.

The VLAN tagged SRIOV packet interfaces are unable to ping endpoint Gateway IPs in the VMware platform because of an issue with VMware.

Performing a Heat Stack Update when userdata is Updated with SSH Keys

When upgrading SBC SWe cloud instances to release 9.2.1, you must update your Heat template userdata section to include mandatory SSH key information. An issue in OpenStack requires that you use the stack-update process rather than re-launch after updating the template, which leads to a new UUID for the instance. As a result, you must regenerate and apply new license bundles to the upgraded instances during the upgrade.

Refer to Upgrading SBC SWe N:1 HA Nodes on OpenStack using Heat Templates for the relevant procedure.

MOP to increase vCPUs Prior to Upgrading SBC SWe on VMware or KVM Hypervisor (9.2.3R2)

The SBC Core release 9.2 includes a feature that extends the use of hyper-threading to SBC SWe when it is installed on either the VMware or KVM Hypervisor platform. To take advantage of the performance improvements provided by hyper-threading, you must increase (double) the number of vCPUs configured in the VM prior to software upgrade. When upgrading, modify the upgrade process to incorporate the following additional steps: If upgrading SBC SWe KVM Hypervisor or VMware from pre-07.01.00R000 release to 07.01.00R000 or higher:

If upgrading vCPUs from less than 10 to 10 or more, use the procedure below

> **Note**
> This procedure requires shutdown of both SBCs, Ribbon recommends that you perform this procedure during a maintenance window.

1. On the VMware platform only, before beginning the upgrade, disable the CPU reservation check inside the guest by renaming the file: vmware-toolbox-cmd. For example, issue the following command:
   mv /usr/bin/vmware-toolbox-cmd /usr/bin/vmware-toolbox-cmd.bak
2. Stop standby SBC by issuing "sbxstop". Wait until the SBC processes stop.
3. Shutdown the standby SBC by issuing "poweroff" command.
4. Increase vCPU count on the powered off standby SBC.
5. Stop an active SBC by issuing "sbxstop". Wait until the SBC processes stop. Note that this is service affecting since both SBCs are stopped now.
6. Shutdown the active SBC by issuing "poweroff" command.
7. Increase vCPU count on the powered off active SBC.
8. Power on the active SBC. Wait for the SBC to fully start as active.
9. Power on the standby SBC. The SBCs should start as standby and get in sync with an active SBC.

For any other CPU upgrade combination, use the procedure below:

1. On the VMware platform only, before beginning the upgrade, disable the CPU reservation check inside the guest by renaming the file: `vmware-toolbox-cmd` For example, issue the following command:
   `mv /usr/bin/vmware-toolbox-cmd /usr/bin/vmware-toolbox-cmd.bak`
2. For either platform, before starting the upgrade procedure, shutdown the standby VM instance and double the number of vCPUs specified for the VM. Refer to the procedure you used creating a VM that is appropriate for your specific deployment:
   (VMware) Creating a New SBC SWe VM Instance with VMXNET3 (step 7)
   (VMware) Creating a New SBC SWe VM Instance with Direct IO Passthru (step 7)
   (KVM) Creating a New SBC SWe Instance on KVM Hypervisor (step 6)
   (KVM) Creating a New SBC SWe Instance with PCI Pass-Through Device (step 6)
3. After increasing the number of vCPUs, power on the standby instance with the increased number of vCPUs in the same release.
4. Switch over the active instance, so that the standby becomes the new active instance. Don't wait for the standby instance to come up. It may not come up due to the resource mismatch.
5. Shutdown the new standby instance and double its number of vCPUs, as done earlier in step 2.
6. Bring up (power on) the new standby and wait for the active and standby nodes to sync.