CVE-2021-44228: Critical Apache Log4j Remote Code Execution Vulnerability

This Wiki page contains the latest Ribbon information for this vulnerability. Please bookmark this page, and check back regularly for updates.

Published: 13 Dec 2021

Change history

Date	Revision	Description
13 Dec 2021	1.0	First publication

Summary

CVE-2021-44228 is a critical remote code execution (RCE) vulnerability in Apache Log4j 2 (2.0-2.14.1), a common logging framework for Java. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted request to a server running a vulnerable version of log4j. The crafted request uses a Java Naming and Directory Interface (JNDI) injection via a variety of services including:

- Lightweight Directory Access Protocol (LDAP)
- Secure LDAP (LDAPS)
- Remote Method Invocation (RMI)
- Domain Name Service (DNS)

If the vulnerable system uses Log4j to log requests, the exploit will then request a malicious payload over JNDI through one of the services above from an attacker-controlled server. Successful exploitation could lead to RCE.

Ribbon Analysis and Investigation

Log4j is used in several Ribbon products, particularly in Java based web interfaces (e.g. GUIs), that are generally only exposed over the management interfaces and private networks. Ribbon is currently assessing the impacts of this vulnerability across its product portfolio.

Please see the following table for product impact assessments and status. Ribbon will update this table frequently as more information becomes available.

Ribbon assessments cover actively supported products and releases. Assessments against supported product releases may apply to older releases. However, Ribbon cannot guarantee an unsupported release is not impacted, nor can Ribbon provide mitigation and/or resolution for unsupported products and/or unsupported releases.

Product Impact Assessments

Product Name	Vulnerability Assessment	Supported Releases	Impacted Releases	Remediation Plan / Timing	Mitigation	Last Modified Date
GSEC	Impacted	GSEC5.0 GSEC6.0	GSEC5.0 GSEC6.0	Plan to be communicated by Dec 15	Evaluating options to mitigate while waiting for the fix	13 Dec 2021
G6 Management Module (G6MM)	Impacted	13.2.8, 13.2.9, 30.0.0, 31.0.0	13.2.8, 13.2.9, 30.0.0, 31.0.0	Plan to be communicated by Dec 15	Evaluating options to mitigate while waiting for the fix	13 Dec 2021
Intelligent Messaging Manager (IMM)	Impacted	5.0	5.0	Plan to be communicated by Dec 15		13 Dec 2021
VNF Manager (VNFM)	Impacted	20.1.1, 21.x	20.1.1, 21.x	20.1.2 (End of Dec '21) 21.3.1 (End of Dec '21)	VNFM is expected to be operating in a private/OAM network, hence exposure is low. If the risk of exposure is a concern in a private/OAM network, mitigation can be applied. Mitigation MOP will be provided by 12/17.	13 Dec 2021
Insight Element Management System (EMS)	Impacted	12.2.x, 13.2.x, 14.x	13.2.X and 14.X	13.2.5 (End of Dec '21) 14.1.1 (End of Feb '22)	EMS is expected to be operating in a private/OAM network, hence exposure is low. If the risk of exposure is a concern in a private/OAM network, mitigation can be applied. Mitigation MOP will be provided by 12/17.	13 Dec 2021
Ribbon Analytics/DCE	Impacted	20.x, 21.x	20.x, 21.x	22.02 (End of Feb '22)	Ribbon Analytics is expected to be operating in a private/OAM network, hence exposure is low. If the risk of exposure is a concern in a private/OAM network, mitigation can be applied. Mitigation MOP/Patch will be provided by 12/20.	13 Dec 2021

Product Name	Vulnerability Assessment	Supported Releases	Impacted Releases	Remediation Plan / Timing	Mitigation	Last Modified Date
SBC Core (51x0/52x0/5400/7000/SWe)	Impacted	V07.02.05, 8.x, 9.x,10.x	10.1.0R0 only	Plan to be communicated by Dec 15	Mitigation MOP will be provided by 12/14.	13 Dec 2021
C3 Gateway Controller / Genview G9 (EMS)	Not Impacted			N/A		13 Dec 2021
G5 Line Access Gateway (LAG)	Not Impacted			N/A		13 Dec 2021
G5 SIP Emergency Stand-Alone (ESA)	Not Impacted			N/A		13 Dec 2021
G6 Universal Gateway	Not Impacted			N/A		13 Dec 2021
G9 Converged Gateway	Not Impacted			N/A		13 Dec 2021
C15 Compact Softswitch	Not Impacted			N/A		13 Dec 2021
C20 Converged Softswitch	Not Impacted	R20, R21		N/A		13 Dec 2021
CS2100 Converged Softswitch	Not Impacted	SE19		N/A		13 Dec 2021
LD Converged Softswitch	Not Impacted	VzCVM17.2		N/A		13 Dec 2021
GENView Manager (GVMB)	Not Impacted	GVMB5.0 GVMB6.0 GVMB7.0		N/A		13 Dec 2021
C20 Core Billing Manager (CBM/CBMG)	Not Impacted			N/A		13 Dec 2021
Virtual Hosting Environment (VHE) / Application Virtual Environment (AVE	Not Impacted			N/A		13 Dec 2021
NSP	Not Impacted	22.0		N/A		13 Dec 2021
GENView Provisioning & Portals (GVPP)	Not Impacted	10.0		N/A		13 Dec 2021
Genview Billing - Mediation (GVB-M)	Not Impacted	7.0		N/A		13 Dec 2021
GENView Assurance (GVA)	Under Investigation					13 Dec 2021
General Media Server (GMS)	Not Impacted	GMS 14.1		N/A		13 Dec 2021
MEP	Under Investigation					13 Dec 2021
Signaling Platform 2000 (SP2000)	Not Impacted	18.x, 19.x, 20.x		N/A		13 Dec 2021
Application Server (AS)	Not Impacted	13.0 14.1		N/A		13 Dec 2021
Media Application Server (MAS)	Under Investigation					13 Dec 2021
Q10, Q20, Q21 Session Border Controller (SBC)	Not Impacted			N/A		13 Dec 2021
Real-Time Session Manager (RSM) / RSM-Lite	Not Impacted			N/A		13 Dec 2021
Identity Hub (IDH)	Not Impacted	21.10		N/A		13 Dec 2021
STI	Not Impacted	20.06 to 21.09		N/A		13 Dec 2021
DSC 8000	Not Impacted	18.x, 19.x		N/A		13 Dec 2021
DSC SWe	Not Impacted	18.x, 19.x		N/A		13 Dec 2021
DataStream Integrator (DSI)	Not Impacted			N/A		13 Dec 2021
GSX (4000/9000)	Not Impacted			N/A		13 Dec 2021
Media Capture Tool (MCT)	Not Impacted			N/A		13 Dec 2021
PSX (including BRX)	Not Impacted			N/A		13 Dec 2021

Product Name	Vulnerability Assessment	Supported Releases	Impacted Releases	Remediation Plan / Timing	Mitigation	Last Modified Date
Ribbon Automation Framework (RAF)	Not Impacted			N/A		13 Dec 2021
SBC Edge (1000/2000/SWe Lite)	Not Impacted	8.x, 9.x, 11.x		N/A		13 Dec 2021
SGX4000	Not Impacted	10.0.0Rx		N/A		13 Dec 2021
T7000 Intelligent Switching System	Not Impacted	6.4, 7.0		N/A		13 Dec 2021
Tenor Series VoIP Gateways (AX/AF)	Not Impacted			N/A		13 Dec 2021
VX Series Voice Switches (VX 900)	Not Impacted			N/A		13 Dec 2021
EdgeMarc 2900/6000/7000 EdgeMarc 4800 series	Not Impacted	16.2.0, 16.2.1, 16.1.0, 15.8.4, 15.6.1, 14.10.5, 14.8.11, 14.9.7		N/A		13 Dec 2021
EdgeView SCC	Not Impacted	16.2.x		N/A		13 Dec 2021
EdgeView 14x and Report Server	Not Impacted	14.2.2p5		N/A		13 Dec 2021