Security Advisory

For Apache Log4j 1.2 Vulnerability (CVE-2021-4104)

Revised 1/10/22 (ver.1)

JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Keysight has determined that some products contain the vulnerable version of the Log4j package. The R&D teams are working with the highest priority to include resolutions in upcoming versions of the product software. Updates will be posted below as soon as the software is made available on the following download site::

https://support.ixiacom.com/support-overview/product-support/downloads-updates

Vulnerable Products

Product	Mitigation
IxLoad LTE UE	

Keysight has determined that the products listed below are not susceptible to the Log4j (CVE-2021-4104) vulnerability and require no update at this time:

Product	Mitigation
Network Visibility Operating System on Keysight Network Packet Brokers (Vision 7300/7303, Vision ONE, Vision 7816, Vision X, Vision E100, Vision E40, Vision E10S) - software v4.x and 5.x	Uses a non-vulnerable version of Log4j (v2.5)

Network Visbility Operating System on Keysight Network Packet Brokers NTO 5288/5293 AND ControlTower (5260, 5263, 5268) - software v4.x	Uses a non-vulnerable version of Log4j (v2.5)
Network Visibility Operating System on Keysight Network Packet Brokers 3.x (211x, 5204/5236/5273/5288/5293/GSC 7433 + Backup Server)	NVOS does use Log4j 1.2.15 but is not vulnerable for 2 reasons - Customers do not have access to modify the NVOS log4j config file AND NVOS does not use JMSAppender. NVOS uses only RollingFileAppender from the 1.2.15 jar.
Visibility Application Module Operating System for either Vision ONE (MV1-VAM) OR Vision X (MVX-AM4-PC)	Mako OS does NOT include Log4j.
AppStack on 7300, Vision ONE and the TradeVision platform	AppStack uses Log4j 1.2.15 but is not vulnerable. Customers do not have access to modify the AppStack log4j config file and JMSAppender is not used.
AppStack on Vision X	AppStack uses Log4j 1.2.15 but is not vulnerable. Customers do not have access to modify the AppStack log4j config file and JMSAppender is not used.
Vision X Decryption, Inline SSL [SUB-VX-ASSL] Vision One Decryption Active SSL [LIC-ASSL-XXXX]	Uses a non-vulnerable version of Log4j (v2.7)
Vision X Decryption, Out of Band SSL [SUB-VX-PSSL] Vision One Decryption Passive SSL [LIC-ASSL-XXXX]	Uses a non-vulnerable version of Log4j (v2.7)
Vision X Application Module (MVX-AM4-PC) running any of the MobileStack SW License Packages, including: LIC-VX-MS2C, LIC-VX-GTP or LIC-VX-GTPFD2C	Uses a non-vulnerable version of Log4j (v2.7)
Visibility Application Module with SIP/RTP Correlation SW Package [MV1-MS-SRC]	Uses a non-vulnerable version of Log4j (v2.7)
CloudLens 6.0 forward	Not affected, we are NOT using log4j v1.2
CloudlLens Self-Hosted/vTap Capability	Not affected, we are NOT using log4j v1.2
CloudLens with AppStack (sometimes vATIP/Virtual AppStack)	AppStack uses Log4j 1.2.15 but is not vulnerable. Customers do not have access to modify the AppStack log4j config file and JMSAppender is not used.
CloudLens vPB (5G SBI NetService)	Not affected, we are NOT using log4j v1.2
Cloudlens vPB	vPB 2.1.0 standalone does not use Log4j
Hawkeye	Not affected, we are NOT using log4j v1.2
Access Products: iBypass 40-10, iBypass 3, iBypass HD, iBypass 10G, iBypass100G, iBypass 1, iBypass2, iLinkAggregator, Director, xStream, xFilter, xBalancer, xDirector, iBypass VHD, iBypass DUO, ixProbe, IxBPCU3, IxTP-CU3,ISIP	These products do not use Java.

Timekeeper	Timekeeper doesn't use log4J
VisionE1S Endpoint	Vision E1S Endpoint does not use Lo4j
Vision E1S - Hawkeye	Not affected, we are NOT using log4j v1.2
Dell Vision Appliance Module used for Hawkeye	Not affected, we are NOT using log4j v1.2
T1000 Industrial Packet Broker	Java isn't used
UHD100T32	
IxNetwork	
IxLoad	
BPS	
IxOS	
IxVM ((IxExplorer VE, IxNetwork VE, IxLoad VE)	
CyPerf	
Threat Simulator	
Network Emulator II	
Network Emulator 100G+	
IxVerify	
Cloud Peak	
TrafficRewind	
ThreatARMOR	
IxSuiteStore	
IxNetworkWeb	
APS (Eagle)	
IxVeriwave	
IxCatapult	
IxLoad 5G (DuSIM, CoreSIM)	
5G LoadCore	
RICtest	Running v1.2 but vulnerability is not exposed.
CuSIM	Running v1.2 but vulnerability is not exposed.
RuSIM, UeSIM	
BreakingPoint Cloud	
IOT Security	
IxChariot (web edition and desktop edition)	
BPS-VE	
Hawkeye and/or Chariot endpoints (XR2000, XRPi, XR2000_VM, XRVM, IxProbe, E1S)	
IxANVL	

More Information

In order to view the latest Keysight Test and Visibility Product Security Advisories,

visit our page https://support.ixiacom.com/support-services/security-advisories

or, for automated notifications, subscribe to our rss feed.

To report a cyber security issue on a Keysight product please go here.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES