Security Advisory

Vulnerability in Apache Log4j Affecting Poly Systems

Last Update: 23-Feb-2022 – 09:00 Central Time
Initial Public Release: 13-Dec-2021
Advisory ID: PLYGN21-108

CVE ID: CVE-2021-44228
CVSS Score: 10.0
CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Vulnerability Summary

A critical remote command execution (RCE) vulnerability in Apache Log4j (CVE-2021-44228) was publicly disclosed on December 9th, 2021. Apache has released a patch for vulnerable versions.

Upon notice of the vulnerability, Poly's incident response process was initiated and we have been conducting a thorough investigation to determine which, if any Poly products and services might be subject to this vulnerability.

This effort is a top priority for Poly and we will continue to update this advisory as more information becomes available.

As this is an ongoing investigation, please note that information related to any product or service may be subject to change.

Any product not listed below is still under investigation to determine whether they are affected by this vulnerability.

Product Status

The following have been identified as affected product or service and includes the dates and versions of which we are currently aware (subject to change as investigation continues). If no date or version is currently listed for an affected product or service, we will update this bulletin when our evaluation is complete, and the information is available.

Product	Fix Availability
Poly Clariti Core/Edge (a.k.a. DMA/CCE) - 9.0 and above	- 14-Dec-2021 - Manual configuration change available. Please contact Poly Support - CCE (a.k.a. DMA) 10.1.0.2 released
Poly Clariti Relay version 1.x	Clariti Relay 1.0.2 – released
Poly RealConnect for Microsoft Teams and Skype for Business	Mitigations Complete
Cloud Relay (OTD and RealConnect hybrid use case)	Mitigations Complete
Plantronics Manager	Mitigations Complete
Plantronics Manager Pro	Mitigations Complete

Products Identified as Not Vulnerable

Headsets
Wireless and Wired Headsets

Phones and Speakerphones
VVX 150/250/350/450
VVX 150/250/350/450 Obi Software
VVX 101/201/300/310/301/311/400/410/401/411/500/501/600/601
CX5100/CX5500
Poly Rove DECT
SoundStation
SoundStation IP
SoundPoint IP
VoiceStation
Obi 300/302/312/504/508
VVX D230
Poly Edge B10/B20/B30
CCX 400/500/600/700

Video Conferencing
ATX300
CX7000/CX8000
Poly G7500
Poly X30/X50/X70
Poly G10-T/G40-T/G85-T
Polycom RealPresence Group Series Family
Polycom RealPresence Immersive Studio
Polycom HDX Family
Polycom Pano
Poly OTX100/OTX300
Poly OTX Studio
Polycom Companion App
Polycom Content App
Trio C60
Trio 8500/Trio 8800

Trio 8300
Trio VisualPro
Visual+
G200
RealPresence Centro
RealPresence Debut
Polycom ISDN Gateway
Polycom VBP 7301
Software and Services
Poly Clariti Manager (RealPresence Resource Manager / RPRM)
Poly RealPresence Collaboration Server (RPCS/RMX)
Poly Clariti App
Poly Content Connect
Poly RealPresence Desktop
Poly RealPresence Mobile

Poly Workflow Server
Poly Workflow Lite
RealPresence Distributed Media Application (DMA 6.x and below)
Poly Lens
PDMS-SP
PDMS-E
Cloud-OTD
RealPresence Access Director (RPAD)
Zero Touch Provisioning Service (ZTP)
Polycom RealAccess
RealPresence Web Suite (RPWS)
Plantronics Hub Desktop (Windows)
Plantronics Hub Desktop (Mac)
Plantronics Hub Mobile (iOS)
Plantronics Hub Mobile (Android)
BToE for VVX

Plantronics Status Indicator Companion
PC Audio Connector
Peripherals
EagleEye Director II
EagleEye IV
EagleEye Mini
EagleEye Cube
Poly Studio E70
Poly Studio
Poly P5
Poly P15
Poly P21
Poly TC8
EagleEye Producer
RealPresence Touch

Eagle Eye IV USB
Poly IP Mic
Poly IP Mic Adapter
Poly IP Ceiling Microphone

Solution

Poly recommends customers upgrade to appropriate software version or later as established in the product table.

https://support.polycom.com/PolycomService/home/home.htm

Implement Alternative Controls for Products/Services until Patches are Available for Deployment

It is recommended to implement strong network security practices and monitor network connections for any unauthorized connections.
In addition, monitoring logs for indications of exploitation is encouraged as well.
Ensure that any alerts from a vulnerable product or service are actioned immediately.
Report incidents promptly to law enforcement and to Poly as provided below.

Details

CVE-2021-44228: Apache Log4j
Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

CVE-2021-45046: Apache Log4j

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack. Log4j 2.15.0 makes a best-effort attempt to restrict JNDI LDAP lookups to localhost by default. Log4j 2.16.0 fixes this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-45046

CVE-2021-45105: Apache Log4j

Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0 and 2.12.3.

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-45105

CVE-2021-44832: Apache Log4j

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-44832

CVE-2022-23307

CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.

Source: https://nvd.nist.gov/vuln/detail/CVE-2022-23307

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Polycom Technical Support – either call 1-800-POLYCOM or visit: https://support.polycom.com/content/support/security-center.html For the latest information.

Revision History

Version	Date	Description	Status
1.51	02/23/2022	Updated product status Added CVE-2022-23307	Interim
1.50	01/07/2022	Updated product status Added CVE-2021-44832	Interim
1.49	12/24/2021	Updated product status and patch availability	Interim
1.48	12/22/2021	Updated product status	Interim
1.48	12/21/2021	Updated product status	Interim
1.47	12/20/2021	Updated product status	Interim
1.46	12/18/2021	Updated product status Added CVE-2021-45105	Interim
1.45	12/17/2021	Updated product status	Interim
1.44	12/17/2021	Updated product and services status	Interim
1.43	12/16/2021	Updated product status	Interim
1.42	12/16/2021	Modified Last update time format	Interim
1.41	12/16/2021	Updated product status, Vulnerability Summary Added update revision to top of document Updated CVE-2021-44228 Detail Added CVE-2021-45046	Interim

1.4	12/15/2021	Updated product status, Vulnerability Summary and Alternative Controls sections	Interim
1.3	12/15/2021	Updated product status and added products not included in prior releases	Interim
1.2	12/14/2021	Updated status and added products	Interim
1.1	12/14/2021	Updated status and added products	Interim
1.0	12/13/2021	Initial Public Release	Interim