AVAYA

Product Support Notice

PSN #	PSN005945u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 15-Dec-21. This is issue #06, published date: 23-Feb-22.		Severity/risk level	High	Urgency	Immediately
Name of problem	Avaya Callback Assist (CBA) Log4j vulnerabilities				

Products affected

Avaya Callback Assist (CBA), 4.7.x, 5.0.0.x and 5.0.1.x.

Problem description

Avaya is aware of the recently identified Apache Log4J vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2021-4104, CVE-2022-23302, CVE-2022-23305, CVE-2022-23307) and is conducting impact assessments across its portfolio, identifying opportunities for temporary mitigations, if possible, and developing plans for remediation. Reference the *Avaya Product Security* - ***Apache Log4J Vulnerability - Impact for Avaya products*** on support.avaya.com for updates

Avaya Callback Assist (CBA), 5.0.0.x and 5.0.1.x Reporting Servers are impacted by the Log4j2 vulnerabilities (CVE-2021-44228, CVE-2021-45046) and are not impacted by CVE-2021-45105, CVE-2021-44832, CVE-2021-4104, CVE-2022-23302, CVE-2022-23305, CVE-2022-23307.

Avaya Callback Assist (CBA), 5.0.0.x and 5.0.1.x Single Server, Application Servers and Database Servers run Log4jv1. The internal analysis has determined that these Servers of these releases are not vulnerable to the related Log4j1x vulnerabilities, but in order to prevent any possible risk, we are preparing a patch to remove the JMS appender, JDBC appender and Chainsaw from Log4jv1 distribution.

Avaya Callback Assist (CBA), 4.x run Log4jv1, but not Log4j2, and are not susceptible. The internal analysis has determined that these Servers of these releases are not vulnerable to the related Log4j1x vulnerabilities, but in order to prevent any possible risk we are preparing a patch to remove JMS appender, JDBC appender, and Chainsaw from Log4jv1 distribution, and set strict permissions to access to Log4j configuration files.

Please only follow documented procedures described in this PSN to resolve this issue.

This PSN will be updated as more information is available.

Resolution

We released a patch to upgrade log4j v2 to 2.17.1. PLDS id is CBA0000000117

We have published patches to remove the JMS appender, JDBC appender, and Chainsaw from Log4jv1 distribution for CBA 5.0.0.x, CBA 5.0.1.x, and CBA 4.7.1.1 Core servers and set strict permissions to access Log4j configuration files for CBA 4.7.1.1.
CBA 4.7.1.1 patch PLDS id is CBA0000000123
CBA 5.0.X patch PLDS id is CBA0000000124

All 3 patches are available from the download page https://support.avaya.com/downloads/download-details.action?contentId=1399840883321&productId=P0536&releaseId=5.0.x

Remarks

Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 17, 2021: Adding information about the patch to the Resolution section. Adding a new step (#5) to workaround.
Issue 3 – December 22, 2021: Adding information about CVE-2021-45105 no impact.
Issue 4 – January 17, 2022: Adding information about CVE-2021-44832, CVE-2021-4104 no impact.
Issue 5 – February 1, 2022: Adding information about Log4j1 vulnerabilities.
Issue 6 – February 23, 2022: Adding information about Log4j1 patches.

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Always

Download

n/a.

Patch install instructions	Service-interrupting?
n/a	Yes

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23302
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23305
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23307

Reference https://logging.apache.org/log4j/2.x/security.html
Reference https://logging.apache.org/log4j/1.2/

Avaya Security Vulnerability Classification

Reference www.avaya.com/emergencyupdate

Mitigation

As noted in this PSN.

If you require further information or assistance, please contact your Authorized Service Provider or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.