Product Support Notice

PSN #	PSN005952u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.		
Original publication date: 15-Dec-21. This is issue #03, published date 06-Jan-22.	Severity/risk level	High	Urgency	Immediately
Name of problem	PSN005952u – Avaya Aura Call Center Elite Multichannel Log4j vulnerabilities			

Products affected

Avaya Aura Call Center Elite Multichannel, 6.6 and its service packs

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) 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 Aura Call Center Elite Multichannel, 6.6 and its service packs are impacted by the Log4j2 vulnerabilities.
These releases use JRE 8u45 and some libraries of log4j2 as part of EMC's CSPortal WebApp.

Avaya Aura Call Center Elite Multichannel, 6.6 and its service packs are running Log4j 1.x that are not susceptible.

Internal analysis has determined that Avaya Aura Call Center Elite Multichannel, 6.6 and its service pack releases are not vulnerable to the associated vulnerability CVE-2021-4104 (Log4j 1.x JMSAppender) although Log4j 1.x is used in the software. This is because JMSAppender is not used in any of the log4j configurations for EMC's CSPortal.

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

This PSN will be updated as more information is available.
Ensure that you are signed up for Avaya E-notifications so that you will be notified when new issues of this PSN are posted.

Resolution

The upcoming service pack will install the latest binaries for log4j2 and support latest JRE for CSPortal WebApp.

Workaround or alternative remediation

The workaround involves two parts. For CSPortal WebApp, replacing log4j2 files of version 2.2 with 2.17.1 or greater and to update JRE from 8u45 to 8u121 or higher. Stop CSPortal Service before performing these steps.

Log4j2 part:

1. Take a backup and delete log4j-api-2.2.jar and log4j-core-2.2.jar from CSPortal WebApp folders. Default location is C:\Program Files\Avaya\Avaya Chat Server Portal\CSPortalWebApp\csportalwebapp\csportal\WEB-INF\lib
2. Download log4j 2.17.1 and place log4j-api-2.17.1.jar and log4j-core-2.17.1.jar in the folder accessed in above step.
   Note: We used https://logging.apache.org/log4j/2.x/download.html to download apache-log4j-2.17.1-bin

JRE update part:

1. Take a backup of jre folder from CSPortal WebApp folders. Default is C:\Program Files\Avaya\Avaya Chat Server Portal\CSPortalWebApp\jre
2. Delete all the contents in the above-mentioned path
3. Now install JRE (8u121 or higher) as mentioned in 'CSPortal Web API Developer's Guide For Elite Multichannel' guide
4. Please ensure that JCE policies are applied
   Note: we used Zulu 8u312b07 jre for this

Remarks

PSN Revision History
Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 21, 2021: Updates to refer to CVE-2021-45046 and CVE-2021-45105. Upgrading log4j2 to log4j 2.17.0
Issue 3 – January 6, 2022: Updates to refer to CVE-2021-44832, CVE-2021-4104. Upgrading log4j2 to log4j 2.17.1

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://logging.apache.org/log4j/2.x/security.html

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.