Product Support Notice

PSN #	PSN020559u

Original publication date: 13-Jan-22. This is issue #03, published date: 22-Feb-22.

Severity/risk level	High	Urgency	Immediately

Name of problem	PSN020559u - Avaya Aura® Communication Manager Log4j vulnerabilities

Products affected

Avaya Aura® Communication Manager, All Releases

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.

- All Communication Manager releases are not impacted by the Log4j 2.x vulnerabilities as Log4j 2.x is not present.
- Communication Manager releases <8.1.0 do not contain Log4j 1.x.
- Log4j 1.x was introduced in Communication Manager 8.1.0 but was never utilized.
- Communication Manager releases 8.1.0 – 8.1.3.3 and 10.1.0.0 will be flagged on security scans for the presence of Log4j 1.x even thought it is not utilized.
  - Internal analysis has determined that Communication Manager releases are not vulnerable to the associated vulnerability CVE-2021-4104 (Log4j 1.x JMSAppender) although Log4j 1.x is present in the software. This is because JMSAppender is not used in any of the log4j configurations for Communication Manager.
  - Internal analysis has determined that Communication Manager releases are not vulnerable to the associated vulnerability CVE-2021-44832 with respect to Log4j 2.x or Log4j 1.x as JndiLookup is not present in the classpath.
  - Internal analysis has determined that Communication Manager releases are not vulnerable to the associated vulnerability CVE-2022-23302 (Log4j 1.x JMSSink) although Log4j 1.x is present in the software. This is because JMSSink is not used in Communication Manager.
  - Internal analysis has determined that Communication Manager releases are not vulnerable to the associated vulnerability CVE-2022-23305 (Log4j 1.x JDBCAppender) although Log4j 1.x is present in the software. This is because JDBCAppender class is not used in Communication Manager.
  - Internal analysis has determined that Communication Manager releases are not vulnerable to the associated vulnerability CVE-2022-23307 (Log4j 1.x Chainsaw) although Log4j 1.x is present in the software. This is because Chainsaw classes are not used in Communication Manager.

This PSN will be updated as more information becomes 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

No release of Communication Manager contains Log4j 2.x.

Log4j 1.x was introduced in 8.1.0, but was never utilized.
Since security scans may flag the presence of Log4j 1.x files, Avaya is completely removing Log4j 1.x.

All instances of Log4j 1.x have been removed from Communication Manager 8.1.3.4 as it is not utilized.
The same action will be taken in the next service pack for CM 10.1.0.x which has a tentative target date of mid-April, 2022.

Workaround or alternative remediation

N/A

Remarks

PSN Revision History:
Issue 1 – January 13, 2022: Initial publication.
Issue 2 – February 3, 2022: Updated for CVE-2022-23302, CVE-2022-23305, CVE-2022-23307
Issue 3 – February 22, 2022: Updated to announce removal of Log4j 1.x from 8.1.3.4 and next 10.1.0.x Service Pack.
.

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	No

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

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.

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.