Product Support Notice

PSN #	PSN005958u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 15-Dec-21. This is issue #04, published date: 03-January-22.

Severity/risk level	High	Urgency	Immediately

Name of problem PSN005958u– Avaya Operational Analyst Log4j2 vulnerability (CVE-2021-44228).

Products affected

Avaya Operational Analyst, 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) 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 Operational Analyst, all releases are running Log4jv1 that are not susceptible if JMSAppender is not configured (not configured in OA OOTB). It is possible to exploit using JMSAppender as configuration settings could make JNDI function the same as it does in log4j 2.x. (CVE-2021-4104).

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

No resolution is needed. See *Workaround or alternative remediation* section.

Workaround or alternative remediation

JMSAppender should not be configured. Initially, it is not configured in OOTB version. To make sure it was not configured later – check Log4J configuration file [Avaya]\BI\data\admin\DataExportConfig.properties. If the appender is configured – remove it from Log4J configuration file and restart Data Export Utility component.

Remarks

Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 17, 2021: Added info related to CVE-2021-45046.
Issue 3 – December 21, 2021: Added info related to CVE-2021-45105.
Issue 4 – January 3, 2022: Added info related to CVE-2021-44832 and CVE-2021-4104.

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.