



Product Support Notice

© 2022 Avaya Inc. All Rights Reserved.

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 #05, published date: 01-Feb-22.

Severity/risk level

High

Urgency

Immediately

Name of problem PSN005958u– Avaya Operational Analyst Log4j2 vulnerability

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](#), [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 Operational Analyst, all releases are running Log4Jv1, so it is not affected by Log4J2 vulnerabilities [CVE-2021-44228](#), [CVE-2021-45046](#), [CVE-2021-45105](#), [CVE-2021-44832](#).

Internal analysis has determined that OA 7.3.* 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 Operational Analyst by default. We recommend checking all log4j.xml files on your IC systems to make sure that this appender has not been added manually.

Internal analysis has determined that OA 7.3.* releases are not vulnerable to the associated vulnerability [CVE-2022-23302](#) (Log4j 1.x JMSSink) although Log4j 1.x is used in the software. This is because JMSSink is not used or configured in any of the log4j configurations for Operational Analyst by default. We recommend checking all log4j.xml files on your IC systems to make sure that this appender has not been added manually.

Internal analysis has determined that OA 7.3.* releases are not vulnerable to the associated vulnerability [CVE-2022-23305](#) (Log4j 1.x JDBCAppender) although Log4j 1.x is used in the software. This is because JDBCAppender is not used or configured in any of the log4j configurations for Operational Analyst by default. We recommend checking all log4j.xml files on your IC systems to make sure that this appender has not been added manually.

Internal analysis has determined that OA 7.3.* releases are not vulnerable to the associated vulnerability [CVE-2022-23307](#) (Log4j 1.x Chainsaw) although Log4j 1.x is used in the software. This is because Chainsaw is not used or configured in any of the log4j configurations for Operational Analyst by default.

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

The actions can be implemented by Customer/Partner.

- For log4j version 1.x (All IC Releases), vulnerable appenders are not configured in OOTB IC packages.

CVE	Mitigation
<u>CVE-2021-4104</u>	Ensure JMSSAppender is not used in logging configuration settings. Disable the log4j feature that allows "to load a remote configuration file or to configure the logger through the code".
<u>CVE-2022-23302</u>	- Comment out or remove JMSSink in the Log4j configuration if it is used - Remove the JMSSink class from the server's jar files. For example: <code>zip -q -d log4j-*.jar org/apache/log4j/net/JMSSink.class</code>
<u>CVE-2022-23305</u>	- Comment out or remove JDBCAppender in the Log4j configuration if it is used - Remove the JDBCAppender class from the server's jar files. For example: <code>zip -q -d log4j-*.jar org/apache/log4j/jdbc/JDBCAppender.class</code>
<u>CVE-2022-23307</u>	Avoid using Chainsaw to view logs, and instead use some other utility, especially if there is a log view available within the product itself. - Remove the Chainsaw classes from the log4j jar files. For example: <code>zip -q -d log4j-*.jar org/apache/log4j/chainsaw/*</code>

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.

Issue 5 – February 1, 2022: Updated *Problem Description* and *Workaround* sections according to new found vulnerabilities CVE-2022-23302, CVE-2022-23305, CVE-2022-23307.

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

n/a

Service-interrupting?

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.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.