Product Support Notice

PSN #	PSN005944u

Original publication date: 15-Dec-21. This is issue #06, published date: 24-Mar-22.

Severity/risk level	High	Urgency	Immediately

Name of problem PSN005944u – Proactive Outreach Manager (POM) - Log4j vulnerabilities.

Products affected

Proactive Outreach Manager (POM) releases 3.1.3.x, 4.0.x, 4.0.1.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.

Proactive Outreach Manager releases 4.0.x, 4.0.1.x are impacted by the Log4j vulnerability (CVE-2021-44228).

Proactive Outreach Manager is not susceptible to Log4j vulnerability(CVE-2021-45105) as context lookup is not used in Log4j configuration.

Proactive Outreach Manager is not susceptible to Log4j vulnerability(CVE-2021-45046) as JNDI Lookup is not used in Log4j configuration.

Proactive Outreach Manager is not susceptible to Log4j vulnerability(CVE-2021-44832) JDBC Appender is not used and permissions are strict to application owners.

Proactive Outreach Manager is not susceptible to Log4j vulnerability(CVE-2021-4104 (Log4j 1.x JMSAppender) because JMSAppender is not used in any of the log4j configurations.

Internal analysis has determined that Proactive Outreach Manager 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 Proactive Outreach Manager by default.

Internal analysis has determined that Proactive Outreach Manager 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 Proactive Outreach Manager by default.

Internal analysis has determined that Proactive Outreach Manager 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 Proactive Outreach Manager by default.

Please only follow documented procedures described in this PSN to resolve this issue for the impacted releases. Note that rollback of the earlier workaround mentioned in Issue #3 and earlier is not needed if already implemented.

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

Upgrade to Proactive Outreach Manager 4.0.1 Patch 3(POM401Patch03.zip; PLDS ID POM000000194).

Workaround or alternative remediation

None. Please upgrade and apply patches as specified in resolution section if you are using any of Proactive Outreach Manager releases 4.0.x, 4.0.1.x.

Remarks

Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 17, 2021: Revised publication.
Issue 3 – December 21, 2021: Revised publication.
Issue 4 – January 5, 2022: Revised publication.
Issue 5 – February 1, 2022: Revised publication.
Issue 6 – March 24, 2022: Revised publication.

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.