Product Support Notice

PSN #	PSN005935u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 15-Dec-21. This is issue #06, published date: 14-Jan-2022.

Severity/risk level	High	Urgency	Immediately

Name of problem PSN005935u – Avaya Meetings® Management Log4j vulnerabilities.

Products affected

Avaya Meetings® Management 9.1.x; previously known as Equinox® Management 9.1.x

Problem description

Avaya is aware of the recently identified Apache Log4j 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.

- Equinox® Management release 9.1 FP9 and earlier are not impacted by the Log4j2 vulnerabilities CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 and CVE-2021-4104.
- Equinox® Management releases 9.1.9 SP1 and later, and Meetings® Management releases 9.1 FP11 and later has the following components which are vulnerable to the exploit CVE-2021-44228 only: User Portal / Web Gateway and Meetings Control.

  Avaya has released a security update to address this. Reference the resolution section of this PSN.
- The Management component is running Log4jv1 that are not susceptible.
- Internal analysis has determined that these releases are not vulnerable to the related Log4j1x plus JMSAppender vulnerability.

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

This PSN will be updated as more information is available.

Resolution

Equinox® Management releases 9.1 FP9 and earlier are not impacted by the Log4J vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 , CVE-2021-44832 and CVE-2021-4104), hence no action needed on Equinox® Management versions 9.1 FP9 or earlier.

For Equinox® Management releases 9.1.9 SP1 and later, and Meetings® Management releases 9.1 FP11 and later, two components are impacted by the Log4J vulnerability (CVE-2021-44228) only: User Portal / Web Gateway and Meetings Control.

- For User Portal / Web Gateway in Team Engagement deployments, please see PSN020553u - Avaya Aura® Web Gateway Log4j vulnerabilities) to apply the Service Pack for the specific version.
- For User Portal / Web Gateway in Over The Top deployments, please refer to the Patch Notes section for the download links.
- For Meetings Control please follow the remediation below for any of the versions.

Workaround or alternative remediation

The below workaround for the Meetings Control component is applicable to customers who have root password access to each Management/UCCS server they maintain. For those customers without root access, please contact Avaya Support Services.

In Meetings Control versions 9.1.10.x-9.1.12.x, log4j-core-2.3.jar is packaged in the Meetings Control but is not actually used, so the .jar files can be removed from the server directly using the following command:

- SSH to Meetings Management/UCCS server with pmgradmin user, then escalate to root
- Execute the following command: *rm -f /opt/avaya/uws/jars/log4j-api-2.3.jar /opt/avaya/uws/jars/log4j-core-2.3.jar*
- Restart the server using: *service avaya.uws restart*

Remarks

PSN Revision History:
Issue 1 – December 15, 2021: Initial publication.

Issue 2 – December 15, 2021: Updated affected components.
Issue 3 – December 17, 2021: Updated the contents.
Issue 4 – December 21, 2021: Updated PSN name, clarified affected components, added clarifications in the Resolution section and Workaround section.
Issue 5 – January 7, 2022: Updated to include details about new CVEs.
Issue 6 – January 14, 2022: Updated the PLDS Download IDs in the Patch Notes section.

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Always – utilize VM snapshot; however, multiple copies of snapshots should not be stored on the VM.

Best practice: Wait for a few days (up to a week) to see that the new version performs well and is stable, and then delete all snapshots.

Coordinate and perform these upgrades at a time interval when the conferencing system is not in use.

Download

Obtain software from https://plds.avaya.com/.

- EQMNG000026 – Avaya Meetings Management Server 9.1.10. Log4j Vulnerability SW Security Update
- EQMNG000027 – Avaya Meetings Management Server 9.1.11. Log4j Vulnerability SW Security Update
- EQMNG000028 – Avaya Meetings Management Server 9.1.12. Log4j Vulnerability SW Security Update

Patch install instructions	Service-interrupting?
Important: Install the security update during a maintenance window to avoid service disruption.	Yes
For Upgrades from prior versions, first complete the upgrade or installation and then apply the security update.	
Refer to the Administering Avaya Meetings Management – Chapter 15: Maintaining your Videoconferencing Network.	

Verification

n/a

Failure

Return to backup – VM snapshot.

Patch uninstall instructions

No uninstall. Return to backup – VM snapshot.

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.