Product Support Notice

PSN # PSN005938u

Original publication date: 15-Dec-21. This is issue #05, published date: 20-Jan-2022.

Severity/risk level: High | Urgency: Immediately

Name of problem: PSN005938u – Avaya Meetings® Media Server Log4j vulnerabilities.

Products affected

Avaya Meetings® Media Server (previously known as Equinox® Media Server), All Releases

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.

All Avaya Equinox®/Meetings® Media Server releases (9.0 -> 9.1.12 SP1) have a component vulnerable to the exploit CVE-2021-44228 only: Web Collaboration Server.
Avaya has released a security update to address this. Reference the resolution section of this PSN.

Note: this vulnerability affects only Meetings Media Servers deployed in the following working modes:

- Full Video + Collaboration
- High-Capacity Audio, Multi-Stream Video and Web Collaboration
- Web Collaboration Only

Meetings Media Servers deployed as a WebRTC Gateway / Avaya Media Gateway (in OTT deployments) are not vulnerable.

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

This PSN will be updated as more information is available.

Resolution

Avaya has released a Security Update to address Log4j2 vulnerabilities CVE-2021-44228, updating log4j to version 2.16.0 which has these vulnerabilities addressed by default.
The following Log4j security updates are available in PLDS for downloading by release:

- Avaya Equinox Media Server 9.1.10: PLDS Download ID = EQMS0000021
- Avaya Meetings Media Server 9.1.11 SP1: PLDS Download ID = EQMS0000022
- Avaya Meetings Media Server 9.1.12 SP1: PLDS Download ID = EQMS0000023

Note 1: Avaya Equinox® Media Server releases 9.0 through 9.1.9 SP1 will need to upgrade to release 9.1 FP10 or greater with the latest patch / Service Pack, and then apply the specific log4j security update to mitigate the problem.

Note 2: In order to align all product versions across deployment types and working modes, Avaya will be releasing a consolidated Media Server bundle that will update log4j to version 2.17.1 in all of its components (active or otherwise). It is strongly recommended to apply this security update to all Meetings Media Servers in all working modes as it becomes available.

Workaround or alternative remediation

While Avaya recommends following the steps in the Resolution section of this PSN, as an alternative to the Security Update identified in the Resolution section of this PSN, the remediation outlined below can also be applied to all Equinox/Meetings Media Server R9.1.X versions to mitigate the issue.

Note: The below steps for the Web Collaboration Server component are applicable to customers who have root password access to each Media Server / Web Collaboration server they maintain. For those customers without root access, please contact Avaya Support Services.

- SSH to the Media Server/Web Collaboration Server with pmgradmin user, then escalate to root
- Execute the following command:
  zip -q -d /opt/Avaya/WCS/jars/log4j-core-2.3.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

- Restart WCS using: *service avaya.wcs restart*

Remarks
PSN Revision History: Issue 1 – December 15, 2021: Initial publication. Issue 2 – December 17, 2021: Updated mitigation information Issue 3 – December 21, 2021: Updated PSN name, added SW Fix details in the Resolution section, updated the Workaround section and added Patch notes. Issue 4 – January 7, 2022: Updated with new CVEs information. Issue 5 – January 20, 2022: Added clarification about affected working modes, notification of upcoming bundle patch updating lof4j to 2.17.1.

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/. PLDS Download IDs are referenced in the Resolution section above.

Patch install instructions	Service-interrupting?
Important: Install the security update during a maintenance window to avoid service disruption. For Upgrades from prior versions, first complete the upgrade or installation and then apply the security update. Refer to the Administering Avaya Meetings Media Server – Chapter 5: Load and patch management.	Yes

Verification
The Log4j Vulnerabilities are not directly reproducible. Verify the Software Security Update by verifying that the relevant .jar files have been updated. Before Update: /opt/avaya/WCS/jars/log4j-api-2.3.jar /opt/avaya/WCS/jars/log4j-core-2.3.jar After Update: /opt/avaya/WCS/jars/log4j-core-2.16.0.jar /opt/avaya/WCS/jars/log4j-api-2.16.0.jar

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.