AVAYA

Product Support Notice

PSN #	PSN005938u	

Original publication date: 15-Dec-21. This is issue #07, published date: 04-Apr-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, 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.

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 vulnerability CVE-2021-44228.
In order to align all product versions across deployment types and working modes, this security update is a consolidated Media Server bundle that updates log4j to version 2.17.1 in all of its components (active or otherwise).
Please refer to the Patch Notes section for the 9.1.10/9.1.11/9.1.12 download links.
It is strongly recommended to apply this security update to all Meetings Media Servers in all working modes.

Note: 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.

Alternatively, customers are encouraged to upgrade to the recently released Meetings Server R9.1 FP13 which includes the above fixes for the vulnerabilities. For details, please refer to the Meetings Server R9.1 FP13 download page.

Workaround or alternative remediation

n/a

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.

Issue 6 – February 23,2022: Updated with new CVEs information, updated sections: Resolution, Workaround and Patch Notes.

Issue 7 – April 4, 2022: Updated to clarify that Meetings Server release 9.1.13 includes the security update for these vulnerabilities.

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/.

- EQMS0000024 – Avaya Meetings Media Server 9.1.10 P16. Log4j Vulnerability - Security Update 2
- EQMS0000025 – Avaya Meetings Media Server 9.1.11 SP1. Log4j Vulnerability - Security Update 2
- EQMS0000026 – Avaya Meetings Media Server 9.1.12 GA. Log4j Vulnerability - Security Update 2

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 Media Server – Chapter 5: Load and patch management.

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-2.17.1.jar
/opt/avaya/WCS/jars/log4j-api-2.17.1.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://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.