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 #08, published date: 04-Apr-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](#), [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.

- Equinox® Management release 9.1 FP9 and earlier are <u>not</u> impacted by the Log4j2 vulnerabilities CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2021-4104, CVE-2022-23302, CVE-2022-23305 and CVE-2022-23307.
- Equinox® Management releases 9.1.9 SP1 and later, and Meetings® Management releases 9.1 FP11 and later have a component vulnerable to the exploit CVE-2021-44228 only: User Portal / Web Gateway.

  Avaya has released a security update to address this. Reference the resolution section of this PSN.
- The Management component and Meetings Control component (versions 9.1.9 SP1 and higher) are running Log4jv1 that are not susceptible to these vulnerabilities. The Meetings Control component packs log4j v2.3, but it is never used; thus, while it is unharmful, it may cause some confusion.
- Internal analysis has determined that these releases are not vulnerable to the related Log4j1x plus other vulnerabilities mentioned in this document.
- In order to avoid any confusion, Avaya has released a security update in which log4j version 2.17.1 is used to replace the log4j version 1.x for all the components. This update will also remove the unused log4j v2.3 in the Meetings Control component.

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, CVE-2021-4104, CVE-2022-23302, CVE-2022-23305 and CVE-2022-23307), 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, Avaya has released a Security Update to address Log4j2 vulnerability CVE-2021-44228.
In order to align all product versions across deployment types, this security update is a consolidated Management Server bundle that updates log4j to version 2.17.1 in all of its components (active or otherwise) and removes the unused log4j v2.3 in the Meetings Control component.
Please refer to the Patch Notes section for the 9.1.10/9.1.11/9.1.12 download links.

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.

Note 1: Avaya Equinox® Management 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: 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.

Workaround or alternative remediation
n/a

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.
Issue 7 – February 23,2022: Updated with new CVEs information, updated sections: Resolution, Workaround and Patch Notes.
Issue 8 – 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/.
- EQMNG000029 – Avaya Meetings Management Server 9.1.10. Log4j Vulnerability - Security Update 2
- EQMNG000030 – Avaya Meetings Management Server 9.1.11. Log4j Vulnerability - Security Update 2
- EQMNG000031 – Avaya Meetings Management Server 9.1.12. 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 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://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.