



## Product Support Notice

© 2022 Avaya Inc. All Rights Reserved.

PSN # PSN005936u

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

Original publication date: 15-Dec-21. This is Issue #04, published date: 07- January- 2022. Severity/risk level High Urgency Immediately

### Name of problem

PSN005936u - Avaya Meetings® Streaming and Recording Log4j vulnerabilities (CVE-2021-44228).

### Products affected

Avaya Meetings® Streaming and Recording (previously known as Equinox® Streaming and Recording), All Releases

Avaya Meetings® Recording Gateway (previously known as Equinox® Recording Gateway), 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.

#### Avaya Equinox/Meetings Streaming and Recording

- Equinox® Streaming and Recording releases 9.1 FP5 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® Streaming and Recording releases 9.1 FP8 and later, and Meetings® Streaming and Recording releases 9.1 FP11 and later have a component vulnerable to the exploit (CVE-2021-44228): Manager.

Avaya has released a security update to address this. Reference the resolution section of this PSN.

#### Avaya Equinox/Meetings Recording Gateway

All Avaya Equinox/Meetings Recording Gateway releases (9.0 -> 9.1.12 SP1) have a component vulnerable to the exploit (CVE-2021-44228) on: Web Collaboration Server.

Avaya has released a security update to address this. Reference the resolution section of this PSN.

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 Equinox/Meetings Streaming and Recording

- Avaya Equinox® Streaming and Recording releases 9.1 FP5 and earlier are not impacted by this vulnerability, hence no action is needed for these versions.
- For Equinox® Streaming and Recording releases 9.1 FP8 and later, and Meetings® Streaming and Recording releases 9.1 FP11 and later, Avaya has released a Security Update to address Log4j2 vulnerabilities CVE-2021-44228 and CVE-2021-45046, 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 Streaming and Recording Manager 9.1.10: PLDS Download ID = EQSR0000075
- Avaya Meetings Streaming and Recording Manager 9.1.11 SP1: PLDS Download ID = EQSR0000076
- Avaya Meetings Streaming and Recording Manager 9.1.12 SP1: PLDS Download ID = EQSR0000077

Note: Avaya Equinox® Streaming and Recording releases 9.1 FP8 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.

#### Avaya Equinox/Meetings Recording Gateway

Avaya has released a Security Update to address Log4j2 vulnerabilities CVE-2021-44228 and CVE-2021-45046, 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 Recording Gateway 9.1.10: PLDS Download ID = EQRGW000017
- Avaya Meetings Recording Gateway 9.1.11 SP1: PLDS Download ID = EQRGW000018
- Avaya Meetings Recording Gateway 9.1.12 SP1: PLDS Download ID = EQRGW000019

Note: Avaya Equinox® Recording Gateway 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.

## Workaround or alternative remediation

### Avaya Equinox/Meetings Recording Gateway

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 Equinox/Meetings Recording Gateway R9.1.10.x-R9.1.12.x to mitigate the issue.

Note: The below steps for the Recording Gateway are applicable to customers who have root password access to each Recording Gateway they maintain. For those customers without root access, please contact Avaya Support Services.

- SSH to the Recording Gateway 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 the Recording Gateway using: `service avaya.wcs restart`

## Remarks

PSN Revision History:

Issue 1 – December 15, 2021: Initial publication.

Issue 2 – December 17, 2021: Updated version 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 CVE details.

## Patch Notes

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

### Backup before applying the patch

#### Avaya Equinox/Meetings Streaming and Recording

The Manager backup is performed daily. It's always a good idea to perform a backup prior to an update, so if there are changes in the Manager since the previous day, follow documented procedures to back up the Manager.

#### Avaya Equinox/Meetings Recording Gateway

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.

### Software install instructions

Service-  
interrupting?

#### Avaya Equinox/Meetings Streaming and Recording

No

The Avaya Meetings Streaming and Recording Manager is upgraded using the **assr\_installer** utility included on the server. To upgrade, perform the following on your Avaya Meetings Streaming and Recording appliance which hosts the Manager:

1. Log onto the server
2. Download the Manager update (delivered as a ZIP file)
3. Open a command prompt window
4. Navigate to the folder where you downloaded the component

5. Issue the command: `assr_installer.exe <zip>`

### Avaya Equinox/Meetings Recording Gateway

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

##### Avaya Equinox/Meetings Streaming and Recording

- Verify version information for the Manager component
  - For the 9.1.10 service pack, the Manager version is **9.1.10.100**
  - For the 9.1.11 service pack, the Manager version is **9.1.11.100**
  - For the 9.1.12 service pack, the Manager version is **9.1.13.002**
- Performing basic sanity testing of 5-10 recordings / broadcasts is recommended to ensure normal system operation
- Verify that all logs in the **C:\Program Files\Apache Software Foundation\TomcatXXX\logs** are being generated properly (debug, rest, audit, polling, warn). Note, the Tomcat version is different from release 9.1.10 to releases 9.1.11 and 9.1.12

### Avaya Equinox/Meetings Recording Gateway

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

**Avaya Equinox/Meetings Streaming and Recording:** Re-install previous version of Manager.

**Avaya Equinox/Meetings Recording Gateway:** Return to backup – VM snapshot.

#### Patch uninstall instructions

No uninstall. Re-install previous version of Manager / backup.

## 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](http://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](http://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.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.  
All other trademarks are the property of their respective owners.