Product Support Notice

PSN #	PSN020551u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 14-Dec-21. This is issue #10, published date 03-Feb-22.

Severity/risk level	High	Urgency	Immediately

Name of problem: PSN020551u - Avaya Aura® Application Enablement Services Log4j vulnerabilities

Products affected

Avaya Aura® Application Enablement Services (AES), All Releases

Problem description

See Remarks section for most recent version history.

Jan 4, 2022 – Update: Updated for CVE-2021-4104, CVE-2021-44832 and Super Patches for 8.1.3.2 and 8.1.3.3 to replace the hotfix AES_28416_8.1.3.x.bin.

Dec 24, 2021 -- Critical Update: ~~An issue has been identified with the `AES_28416_8.1.3.x.bin patch` that impacts the OAM interface. After application of the hotfix, the **User Management Tab** is not accessible/visible on the AES OAM interface. Additional steps are required after application of the 8.1.3.x hotfix to ensure the OAM interface is fully functional. Reference the Resolution and Patch Install Sections of this PSN for details. The Super Patch for AES 10.1 does not have this issue.~~*Hot fix for 8.1.3.x has been deprecated.*

Avaya is aware of the recently identified Apache Log4j vulnerabilities (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.

- AES versions earlier than 8.1.3.2 are not impacted by the Log4j 2.x.
- AES versions 8.1.3.2, 8.1.3.3 and 10.1 are vulnerable to the exploit and development and has provided software updates noted in the Resolution section of this PSN.
- Internal analysis has determined that AES 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2021-45105.
- Internal analysis has determined that AES 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2021-4104 (Log4j 1.x JMSAppender) although Log4j 1.x is used in the software. This is because JMSAppender is not used in any of the log4j configurations for AES.
- Internal analysis has determined that AES 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2021-44832.
- Internal analysis has determined that AES 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2022-23302 (Log4j 1.x JMSSink) although Log4j 1.x is used in the software. This is because AES does not use remote configuration files for logging. Attackers cannot modify any logging configuration files on AES as the write permissions are restricted. JMSSink is not used in AES.
- Internal analysis has determined that AES 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2022-23305 (Log4j 1.x JDBCAppender) although Log4j 1.x is used in the software. This is because JDBCAppender is not used or configured in any of the log4j configurations for AES.
- Internal analysis has determined that AES 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2022-23307 (Log4j 1.x Chainsaw) although Log4j 1.x is used in the software. This is because AES does not provide any graphical user interface for viewing log entries in log4j. Chainsaw classes form the log4j jar are not used by AES.

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

This PSN will be updated as more information is available.
Ensure that you are signed up for Avaya E-notifications so that you will be notified when new issues of this PSN are posted.

Resolution

The Super Patches listed below for AES 8.1.3.2 and 8.1.3.3 have been created to address Log4j 2.x vulnerabilities CVE-2021-44228 and CVE-2021-45046.
AES 10.1 Super Patch 2 described in **PSN020545u - Avaya Aura® Application Enablement (AE) Services 10.1 Super Patches**, includes Log4j 2.16 and therefore addresses Log4j 2.x vulnerabilities CVE-2021-44228 and CVE-2021-45046.

AES is not susceptible to CVE-2021-4104, CVE-2021-45105, CVE-2021-44832 as noted above.

January 4, 2022: Hot fix AES_28416_8.1.3.x.bin is deprecated and replaced with Super Patches for 8.1.3.2 and 8.1.3.3.
If any Log4j hotfix was previously applied, there is no need to uninstall/remove the hotfix before installing the Super Patch.

Release	Hotfix Available or Super Patch	CVEs Addressed
8.1.3.2	**AES 8.1.3.2 Super Patch 1** **File Name**: aesvcs-8.1.3.2.1-superpatch.bin **File Size:** 22.16 MB (22,694.67 KB) **MD5 Checksum:** fbce414a0eb5458fe6babf38ceb19aa2 **PLDS Download ID:** AES00000898	CVE-2021-44228 CVE-2021-45046 (Not susceptible to CVE-2021-4104, CVE-2021-45105, CVE-2021-44832)
8.1.3.3	**AES 8.1.3.3 Super Patch 1** **File Name**: aesvcs-8.1.3.3.1-superpatch.bin **File Size:** 22.16 MB (22,694.73 KB) **MD5 Checksum:** 3637fee4203d81f2ab41ff1b91178b88 **PLDS Download ID:** AES00000899	CVE-2021-44228 CVE-2021-45046 (Not susceptible to CVE-2021-4104, CVE-2021-45105, CVE-2021-44832)
10.1	**AES 10.1 Super Patch 2 (10.1.0.0.2)** **File Name:** aesvcs-10.1.0.0.2-superpatch.bin **File Size:** 148.75 MB (152,321.45 KB) **MD5 Checksum:** 1cb8cfb887a63fbb3d42423b9f1e5100 **PLDS Download ID:** AES00000897	CVE-2021-44228 CVE-2021-45046 (Not susceptible to CVE-2021-4104, CVE-2021-45105, CVE-2021-44832)

Reference the Patch Notes section of this PSN for installation instructions.

Ensure that you are signed up for Avaya E-notifications so that you will be notified when new issues of this PSN are posted.

Workaround or alternative remediation

N/A.

Remarks

PSN Revision History:
Issue 1 – December 14, 2021: Initial publication.
Issue 2 – December 15, 2021: Updated with hotfixes to address Log4j vulnerabilities for 8.1.3.2, 8.1.3.3.
Issue 3 – December 17, 2021: Updated installation and uninstall instructions with additional details.
Issue 4 – December 21, 2021: Updated with AES 10.1 Super Patch 2 to address Log4j vulnerabilities for 10.1.
Issue 5 – December 21, 2021: Updated with detailed steps for GRHA.
Issue 6 – December 24, 2021: Updated with additional steps required after application of 8.1.3.x hot fix.
Issue 7 – January 4, 2022: Updated for CVE-2021-4104, CVE-2021-44832 and Super Patches for 8.1.3.x to replace the hotfix AES_28416_8.1.3.x.bin.
Issue 8 – January 7, 2022: Updated with md5sum and swversion output example. GRHA note. Reboot not required with Super Patch.
Issue 9 – January 20, 2022: Clarified no need to remove existing Log4j hotfix prior to applying Super Patch.
Issue 10 – February 3, 2022: Updated for CVE-2022-23302, CVE-2022-23305, CVE-2022-23307.

Patch Notes

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

Backup before applying the patch

Always

Download

Always verify the MD5 Checksum after downloading the file from PLDS and after copying the file to the AES Server.

8.1.3.2

AES 8.1.3.2 Super Patch 1
File Name: aesvcs-8.1.3.2.1-superpatch.bin
File Size: 22.16 MB (22,694.67 KB)
MD5 Checksum: fbce414a0eb5458fe6babf38ceb19aa2
PLDS Download ID: AES00000898

8.1.3.3

AES 8.1.3.3 Super Patch 1
File Name: aesvcs-8.1.3.3.1-superpatch.bin
File Size: 22.16 MB (22,694.73 KB)
MD5 Checksum: 3637fee4203d81f2ab41ff1b91178b88
PLDS Download ID: AES00000899

10.1

AES 10.1 Super Patch 2 (10.1.0.0.2)
File Name: aesvcs-10.1.0.0.2-superpatch.bin
File Size: 148.75 MB (152,321.45 KB)
MD5 Checksum: 1cb8cfb887a63fbb3d42423b9f1e5100
PLDS Download ID: AES00000897

Patch install instructions — Service-interrupting?

Notes: Yes

- Super Patch application on a GRHA system is only necessary on the primary server as it will automatically update to the standby.
- If any Log4j hotfix was previously applied, there is no need to uninstall/remove the hotfix before installing the Super Patch.

10.1

Follow the instructions in **PSN020545u - Avaya Aura® Application Enablement (AE) Services 10.1 Super Patches.**

8.1.3.2 and 8.1.3.3 Super Patches

Note:

- The AE Services server is out of service for 20 to 30 minutes while the patch is being applied.
- Best practice is to install the Super Patch during a maintenance window and to always perform a backup prior to installation.

Check the detailed AE Services version.

Use the AE Services Linux console to determine whether the patch has already been applied by executing the **swversion** command on the Command Line Interface (CLI). If the patch has not been applied, proceed with the following steps.

Installing the Patch on the AE Services server
These instructions are applicable for any Super Patch binary. **The example below is for 8.1.3.2.1**

For the VMware or Software Only offers use the following steps to install the patch:

1. Login to the AE Services server using the local Linux console, the service port or SSH.
2. Secure copy the patch file to the **/tmp** directory on the AE Services server.
3. Verify the MD5 Checksum of the patch file.
4. As root user execute the following commands from the Command Line Interface (CLI).

```
cd /tmp
chmod 750 aesvcs-8.1.3.2.1-superpatch.bin
./aesvcs-8.1.3.2.1-superpatch.bin
```

5. Follow the instructions provided.

Verification

Utilize the *swversion* command to ensure the hotfix or Super Patch was installed.

10.1 Super Patch

Follow the instructions in **PSN020545u - Avaya Aura® Application Enablement (AE) Services 10.1 Super Patches.**
The Super Patch is listed under the "Patch Numbers Installed in this system are" section of swversion output.

```
********** Patch Numbers Installed in this system are  **********
10.1.0.0.2
```

8.1.3.2.1 and 8.1.3.3.1 Super Patch

The Super Patch is listed under the "Patch Numbers Installed in this system are" section of swversion output.
The following is an example for 8.1.3.3.1:

```
********** Patch Numbers Installed in this system are  **********
FP8.1.3.0.0.25 (AES 8.1.3)
FP8.1.3.3.0.4 (AES 8.1.3)
8.1.3.3.1
```

Use the following steps to verify successful patch installation:

1. Locally through the service port or remotely by using putty or SSH, start a Linux console session on the AE Services server.
2. Log in as sroot or root.
3. Run the following command to verify the installation of the Super Patch:
   `swversion`
4. Log into the AE Services Management console using a web browser.
5. From the main menu, click **Status**.
6. On the Status page, verify that all previously licensed services are running.
7. Validate the server configuration data, as follows:
   - On the main menu click **Networking**
   - Under **AE Service IP (Local IP)**, verify that the settings are correct.
   - Under **Network Configure**, verify that the displayed settings are correct.
   - Under **Ports**, verify that the settings displayed are correct.
8. Check all of the remaining Management Console pages listed under **AE Services** and **Communication Manager Interface**. Verify that the information is complete and correct.

This completes the installation of the Super Patch.

AE Services server configurations for data changes

Note: Follow this procedure, only if the AE Services server configuration data has changed.
Follow this procedure to restore the AE Services server data:

1. From the main menu of the AE Services Management Console, select **Maintenance > Server Data > Restore**.
   The Management Console displays the Restore Database Configuration screen. The initial state of the Restore Database page provides you with two basic functions:
   - Text box with the **Browse** button, which provides the means to select a backup file to use for the Restore process. Alternatively, you can type a fully qualified name (FQDN) of the backup file in the text box.
   - **Restore** button that starts the Restore process.
2. Click **Browse** and locate the AE Services database backup file that you intend to use
3. Click **Restore**.
   The Management Console redisplays the **Restore Database Configuration** page, with the following message:
   "A database restore is pending. You must restart the Database Service and the AE

Server for the restore to take effect. To restart these services now, click the Restart Services button below."

3. Click **Restart Services**.
   AE Services restarts the Database Service and the AE Services, thereby completing the Restore process.

Failure

Contact Avaya Services

Patch uninstall instructions

10.1

Follow the instructions in **PSN020545u - Avaya Aura® Application Enablement (AE) Services 10.1 Super Patches.**

8.1.3.2.1 and 8.1.3.3.1 Super Patch

These instructions are applicable for any Super Patch binary. **The example below is for 8.1.3.2.1.**
For the VMware or Software Only offers use the following steps to uninstall the patch:

1. Login to the AE Services server using the local Linux console, the service port or SSH.
2. As root user execute the following command from the Command Line Interface (CLI):
   update –e 8.1.3.2.1
3. Follow the instructions provided.
4. Restore server data using the steps provided in the **AE Services server configurations for data changes** section.

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

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.