PSN #	PSN005933u			
Original publication date: 15-Dec-21. This is issue #08, published date: 20-Jan-23.	Severity/risk level	High	Urgency	Immediately
Name of problem	PSN005933u– Avaya Aura Device Services Log4j vulnerabilities			

Products affected

Avaya Aura Device Services, Releases 8.0.1.X, 8.0.2.X ,8.1.3.X, 8.1.4.X, 8.1.5.0, 10.1.0.0

Problem description

Avaya is aware of the recently identified Apache Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, 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.

Log4j 1.x Vulnerabilities

- Internal analysis has determined that AADS 7.X and 8.X and 10.1.0.0 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 Avaya Aura Device Services.

- Internal analysis has determined that AADS 7.X and 8.X and 10.1.0.0 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 JMSSink is not used and not configured in any of the log4j configurations for AADS by default.

- Internal analysis has determined that AADS 7.X and 8.X and 10.1.0.0 releases are not vulnerable to the associated vulnerability CVE-2022-233025 (Log4j 1.x JDBCAppender) although Log4j 1.x is used in the software. This is because JDBCAppender is not used and not configured in any of the log4j configurations for AADS by default.

- Internal analysis has determined that AADS 7.X and 8.X and 10.1.0.0 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 Chainsaw is not used and not configured in any of the log4j configurations for AADS by default.

Log4j 2.x Vulnerabilities

- Avaya Aura Device Services, Releases 7.X and 8.0.0.0 running Log4jv1 that are not susceptible to Log4j2 vulnerability (CVE-2021-44228, CVE-2021-45046 & CVE-2021-45105).

- Avaya Aura Device Services, Releases 8.0.1.X, 8.0.2.X ,8.1.3.X, 8.1.4.X, 8.1.5.0 are impacted by the Log4j2 vulnerability (CVE-2021-44228, CVE-2021-45046). The resolution section provides the details of the fix and the plan.

- Avaya Aura Device Services, Releases 8.0.1.X, 8.0.2.X ,8.1.3.X, 8.1.4.X, 8.1.5.0 are NOT impacted by the Log4j2 vulnerability CVE-2021-45105). The AADS patch mentioned in the Resolution section covers details across various releases.

- Avaya Aura Device Services, Release 10.1.0.0 (GA December 21,2021) is NOT impacted by the Log4j2 vulnerability (CVE-2021-44228, CVE-2021-45046) as it already includes 2.16 log4j jars.

- An updated, mandatory AADS log4j patch Version 2.0 (**AADS000000115)** that replaces the Version 1.0 patch (**AADS000000114)** has been created

This PSN will be updated as more information is available.

Resolution

Updated Jan 7, 2022: **An updated**, mandatory AADS log4j patch Version 2.0 (**AADS000000115)** that replaces the Version 1.0 patch (**AADS000000114)** has been created which fixes all the vulnerabilities in Log4j 2.X - CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 and CVE-2021-44832
.

Root access is NOT required to run this AADS Log4j Version 2.0 patch **AADS000000115 (**Note that version 1 AADS000000114 needed ROOT access)

This updated Version 2 patch (**AADS000000115)** can be applied on top of the Version 1 patch

(**AADS000000114).Important Notes**

1. There is no need to install this patch on AADS 8.1.5.1.5 release, as log4j vulnerabilities are fully addressed in it.
2. Log4j Patch Version 2 (AADS000000115) could be applied to 8.0.1.X,8.0.2.X,8.1.3.X,8.1.4.X,8.1.4.1,8.1.5.0,10.1.0.0 systems
3. Customers who have installed log4j patch Version 1.0 (**AADS000000114)** in 8.0.1.X,8.0.2.X,8.1.3.X,8.1.4.X,8.1.4.1,8.1.5.0,10.1.0.0 releases should proceed to install AADS log4j patch Version 2 (**AADS000000115)**.
4. Patch should be reapplied if AADS systems are upgraded or migrated or rolled back to previous releases.
5. Customer who are in 8.1.4.1 release and already installed patch **AADS000000110** (CVE-2021-44228 & CVE-2021-45046), and log4j patch Version 1.0 (**AADS000000114)** should update the system with AADS log4j patch Version 2 (**AADS000000115)**
6. Customers who are in 8.1.4.1 release and havent installed patch **AADS000000110** (CVE-2021-44228 & CVE-2021-45046), and log4j patch Version 1.0 (**AADS000000114)** should directly proceed to install with AADS log4j patch Version 2 (**AADS000000115)**.

CVE-2021-44832

AADS Release	Impacted by CVE-2021-44832	Resolution Patch for CVE-2021-44832	Date for Patch Release
7.X, 8.0.0.0	NO.	• Not Applicable.	Not Applicable
10.1.0.0	NO. Mitigation Already in place	• **PLDS ID AADS000000115**	1/7/2021
8.1.4.1	NO. Mitigation Already in place	• **PLDS ID AADS000000115**	1/7/2021
8.1.5.X	NO Mitigation Already in place	• **PLDS ID AADS000000115**	1/7/2021

8.0.1. X, 8.0.2. X, 8.1.3.X 8.1.4.X	NO Mitigation Already in place	• **PLDS ID AADS000000115**	1/7/2021

CVE-2021-44228 & CVE-2021-45046

AADS Release	Impacted by CVE-2021-44228 & CVE-2021-45046	Patch for CVE-2021-44228 & CVE-2021-45046	Date for Patch Release
7.X, 8.0.0.0	NO.	• Not Applicable.	Not Applicable
10.1.0.0	NO.	• GA Date is 12/21/2021. • GA load has fix for **CVE-2021-44228 &CVE-2021-45046**	Not Applicable
8.1.4.1	YES	• **PLDS ID AADS000000110** **Recommendation is to use** AADS log4j patch Version 2 (**AADS000000115)**.	12/17/2021
8.1.5.X	YES	• PLDS ID **AADS000000114 - This requires Root access and is deprecated** **The recommendation is to use** AADS log4j patchVersion 2 (**AADS000000115)**.	12/21/2021
8.0.1. X, 8.0.2. X, 8.1.3.X 8.1.4.X	YES	• PLDS ID **AADS000000114 - This requires Root access and is deprecated** **The recommendation is to use** AADS log4j patchVersion 2 (**AADS000000115)**.	12/22/2021

CVE-2021-45105

AADS Release	Impacted by CVE-2021-45105	Patch for CVE-2021-45105	Date for Patch Release
7.X, 8.0.0.0	NO	• Not Applicable.	Not Applicable
10.1.0.0	NO	• AADS is not impacted by CVE-2021-45105 **The recommendation is to use** AADS log4j patchVersion 2 (**AADS000000115)**.	Not Applicable
8.1.4.1	NO	• Patch mentioned in PLDS ID **AADS000000110** covers CVE-2021-44228, CVE-2021-45046 • Patch mentioned in **AADS000000114** covers CVE-2021-44228, CVE-2021-45046 & CVE-2021-45046 **This requires Root access and is deprecated** **The recommendation is to use** AADS log4j patchVersion 2 (**AADS000000115)**.	12/17/2021

8.1.5.X	NO	- PLDS ID **AADS000000114 - This requires Root access and is deprecated** **The recommendation is to use** AADS log4j patchVersion 2 (**AADS000000115)**.	12/21/2021
8.0.1. X, 8.0.2. X, 8.1.3.X 8.1.4.X	NO	- PLDS ID **AADS000000114 - This requires Root access and is deprecated** **The recommendation is to use** AADS log4j patchVersion 2 (**AADS000000115)**.	12/22/2021

Workaround or alternative remediation

Not Applicable.

Remarks

PSN Revision History
Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 21, 2021: Updated the Resolution section with a detailed plan and added CVE-2021-45046 fix details
Issue 3 – December 21, 2021: Updated the PSN with CVE-2021-45105 details and Resolution section with detailed patch release plans
Issue 4 – December 22, 2021: Updated the PSN with Resolution, Download, and Patch install sections with detailed patch details for 8.0.1.X,8.0.2.X,8.1.3.X,8.1.4.X,8.1.4.1,8.1.5.X,10.1.0.0 releases.
Issue 5 – January 7, 2022: Patch Version 2.0 is released and Updated the PSN with CVE-2021-4104 and CVE-2021-44832
Issue 6 – January 13, 2022: Updated the Problem Description section to mention that AADS releases 8.0.1.X, 8.0.2.X,8.1.3.X, 8.1.4.X, 8.1.5.X are NOT impacted by CVE-2021-45105
Issue 7 – February 3, 2022: Updated the "Problem Description" section to include CVE-2022-23302, CVE-2022-23305, and CVE-2022-23307 CVE and its impact.
Issue 8 – January 20, 2023: Updated the "Products affected" section to mention that patch application is needed for AADS release 8.1.5.0 only, as the subsequent release viz. 8.1.5.1 fully addresses all vulnerabilities.

Patch Notes

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

Backup before applying the patch

Always.

A backup or VM snapshot is highly recommended.

Download

Avaya Aura Device Services 8.0.1.X,8.0.2.X,8.1.3.X,8.1.4.X,8.1.4.1,8.1.5.0,10.1.0.0 Patch

1. You may download the file directly from PLDS using PLDS download ID "AADS000000115".
2. Patch would be updated on support site too soon. Once it's approved in support PSN would be updated with details.

Avaya Aura Device Services 8.1.4.1 Patch

Note: Customers can download Patch AADS000000115 alternatively which covers all three vulnerabilities CVE-2021-44228.

CVE-2021-45046, CVE-2021-45046 & CVE-2021-44832

1. You may download the file directly from PLDS using PLDS download ID “AADS000000115”.
2. Patch would be updated on the support site too soon. Once it’s approved in support PSN would be updated with details.

Patch install instructions	Service-interrupting?
	Yes

Avaya Aura Device Services 8.0.1.X,8.0.2.X,8.1.3.X,8.1.4.X,8.1.4.1,8.1.5.0,10.1.0.0 Patch

1. Download the patch as mentioned in the “Download” section.
2. Patch File name is aads-patch-upgradeLog4j.bin.
3. Take a snapshot of the AADS virtual machine. Note that this activity might impact the service.
4. Copy the "aads-patch-upgradeLog4j.bin" to the administrative user's home directory.e.g., If the administrative user is "admin", copy this script to /home/admin/
5. chmod 750 aads-patch-upgradeLog4j.bin
6. Run "aads-patch-upgradeLog4j.bin" using a "sudo" prefix, like this:
   "sudo ./aads-patch-upgradeLog4j.bin----- install

   Refer to README in the patch file for detailed patch information.

Verification

sudo ./aads-patch-upgradeLog4j.bin----- status

Failure

n/a

Patch uninstall instructions

This patch is not reversible. This patch can only be removed by reverting to a snapshot taken before applying the patch.

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 theAvaya 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 REPRESENTATIONSOR 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.