Product Support Notice

PSN #	PSN020553u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 15-Dec-22. This is issue: #07, published date: 03-Mar-22.		Severity/risk level	High	Urgency	Immediately

Name of problem

PSN020553u - Avaya Aura® Web Gateway Log4j vulnerabilities

Products affected

Avaya Aura® Web Gateway (AAWG), 3.7.0.1 – 3.11.0.0

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-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

- AAWG versions earlier than 3.7.0.1 are not impacted by Log4j2 vulnerability CVE-2021-44228.
- AAWG versions 3.7.0.1 and later are susceptible to CVE-2021-44228 and Avaya is releasing Service Packs to address this. Reference the resolution section of this PSN.
- Internal analysis has determined that AAWG (all versions) is not impacted by the following vulnerabilities:
  - CVE-2021-45046 and CVE-2021-45105 because AAWG does not use non-default Pattern Layout with a Context Lookup.
  - CVE-2021-44832 because it is impossible for an attacker to get access to the AAWG log4j configuration.
  - CVE-2021-4104 because AAWG does not use JMSAppender.
  - CVE-2022-23302 because AAWG does not use JMSSink.
  - CVE-2022-23305 because AAWG does not use JDBCAppender.
  - CVE-2022-23307 because AAWG does not use Apache Chainsaw.

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

Avaya has released multiple Service Packs to address the vulnerabilities with Log4j 2.x and most of the Log4j 1.x usages replaced with log4j 2.17.1. Please refer to the Patch Notes section for the download links.

Workaround or alternative remediation

Before the Service Packs, Avaya also released a temporary remediation to address CVE-2021-44228. The remediation is a script which adds property “log4j2.formatMsgNoLookups”. Please note that this remediation is not considered a reliable measure against CVE-2021-44228. It only blocks the most straightforward attack vectors as this page explains (section “Older (discredited) mitigation measures"):
https://logging.apache.org/log4j/2.x/security.html#CVE-2021-44228
Therefore, it is highly recommended to upgrade to one of the Service Packs mentioned in section Patch Notes as soon as possible. The remediation script can still be applied as a temporary measure until the upgrade is done. To get it applied, please contact Avaya Services.

Remarks

PSN Revision History:
Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 16, 2021: Included 3.7.0.1 as a susceptible release, added a clarification in the Resolution section.
Issue 3 – December 17, 2021: Released a Service Pack to address CVE-2021-44228 for Team Engagement.
Issue 4 – December 21, 2021: Updates related to CVE-2021-45046 and CVE-2021-45105.
Issue 5 – December 23, 2021: Released Service Packs to address CVE-2021-44228 for Avaya Meetings 9.1.10, 9.1.11, 9.1.12.

Issue 6 – January 17, 2022: Released new Service Packs for Avaya Meetings and Team Engagement deployments with log4j2 updated to 2.17.0.
Issue 7 – March 03, 2022: Released new Service Packs for Team Engagement deployments with log4j2 updated to 2.17.1 and most of the Log4j 1.x usages replaced with log4j 2.17.1.

Patch Notes

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

Backup before applying the patch
N/A

Download

AAWG 3.11.0.4 for Team Engagement deployment

https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=AAWG000000105

PLDS Download ID: AAWG000000105

AAWG 3.9.1.3 for Team Engagement deployment

https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=AAWG000000102

PLDS Download ID: AAWG000000102

AAWG 3.9.0.4 for Team Engagement deployment

https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=AAWG000000103

PLDS Download ID: AAWG000000103

AAWG 3.8.1.5 for Team Engagement deployment

https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=AAWG0
00104

PLDS Download ID: AAWG000000104

For AAWG systems deployed as a part of Avaya Meetings solution, please see PSN005935u – Avaya Meetings® Management Log4j vulnerabilities.

Patch install instructions	Service-interrupting?
Please follow the standard AAWG upgrade procedure described in the documentation.	Yes

Verification
N/A

Failure
N/A

Patch uninstall instructions
Please follow the standard AAWG rollback/uninstall procedures described in the documentation.

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.

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.