



Product Support Notice

© 2022 Avaya Inc. All Rights Reserved.

PSN # PSN005932u

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: 10-Jan-22. Severity/risk level High Urgency Immediately

Name of problem PSN005932u - Avaya Social Media Hub Log4j2 vulnerabilities ([CVE-2021-44228](#), [CVE-2021-45046](#), [CVE-2021-45105](#), [CVE-2021-44832](#), [CVE-2021-4104](#))

Products affected

[Product Name, Releases]

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](#)) 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 Social Media Hub 1.0 users are not impacted.

Avaya Social Media Hub 1.1 users are only affected if using the Call Center Elite connector.

Avaya Social Media Hub (all releases) with Oceana connector are not impacted.

Avaya Social Connections users are only affected if using the Call Center Elite connector.

Resolution

Solution patches are currently being developed for the CC-Elite Connector to address the vulnerability and the PSN will be updated with the expected release dates.

Any Social Media Hub Customers with CC-Elite Connector will need to apply the solution patches when they are released.

Other Social Media Hub users are not impacted.

Workaround or alternative remediation

As a precaution, please ensure that the elite service is not running:
docker stack rm elite

Remarks

PSN Revision History

Issue 1 – December 15, 2021: Initial publication.

Issue 2 – December 17, 2021: Added info related to CVE-2021-45046.

Issue 3 – December 21, 2021: Added info related to CVE-2021-45105.

Issue 4 – Jan 10, 2022: Added info related to CVE-2021-44832, CVE-2021-4104.

Patch Notes

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

[IF a patch is available, instructions can be included here or simply reference to Resolution section – whatever is cleaner]

Backup before applying the patch

Always

Download

n/a.

Patch install instructions

Service-interrupting?

n/a

Yes

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

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

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.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.

All other trademarks are the property of their respective owners.