



Product Support Notice

© 2021 Avaya Inc. All Rights Reserved.

PSN # PSN005950u Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 15-Dec-21. This is issue #08, published date: 06-Jan-22. Severity/risk level High Urgency Immediately

Name of problem PSN005950u– Avaya Co-Browsing Snap-in Log4j vulnerabilities.

Products affected

Avaya Co-Browsing Snap-in

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 Co-Browsing snap-in deployed on Avaya Breeze™ and uses log4j provided by it. Avaya Co-Browsing snap-in also includes the log4j version 1.x but it is not susceptible and does not use JMSAppender or JNDI configuration.

Table with 4 columns: Co-Browsing version, Breeze Version, Remediation required, and Description. Rows include versions 3.0, 3.2, 3.2.2, 3.3, 3.4, 3.6, 3.6.1, 3.7, and 3.8 with corresponding remediation status and descriptions.

3.8.1	3.8	Yes	Apply patch from Avaya Breeze™ for Log4j2 vulnerabilities mentioned in PSN https://download.avaya.com/css/public/documents/101079448 . Note: Addresses the vulnerability CVE-2021-44228. No fix required for CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 and CVE-2021-4104.
3.8.1.1	3.8.1	Yes	<ul style="list-style-type: none"> Apply patch from Avaya Breeze™ for Log4j2 vulnerabilities mentioned in PSN https://download.avaya.com/css/public/documents/101079448. Note: Addresses the vulnerability CVE-2021-44228. No fix required for CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 and CVE-2021-4104. All deployments on 3.8.1.1 need to upgrade from CoBrowse-3.8.1.1.1290091 to CoBrowse-3.8.1.1.1330096. Note: Fix for vulnerability CVE-2021-44228. No fix required for CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 and CVE-2021-4104.

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

This PSN will be updated as more information is available.

Resolution

The resolution explained below addresses the vulnerabilities CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 and CVE-2021-4104.

- Need to upgrade Avaya Breeze™ and Avaya Co-Browsing releases 3.4 to release 3.7 or later versions.
- Recommended to upgrade Avaya Breeze™ and Avaya Co-Browsing releases 3.6 and 3.6.1 to release 3.7 or later versions.
- Apply Log4j2 vulnerability patches from Breeze for Co-Browsing releases 3.6, 3.6.1, 3.7, 3.8, 3.8.1. Information available on PSN <https://download.avaya.com/css/public/documents/101079448>
- All deployments on 3.8.1.1 need to upgrade from CoBrowse-3.8.1.1.1290091 to CoBrowse-3.8.1.1.1330096.

Workaround or alternative remediation

NA

Remarks

Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 15, 2021: Updated the fix of vulnerability CVE-2021-44228.
Issue 3 – December 15, 2021: Updated the fix of vulnerability CVE-2021-44228.
Issue 4 – December 17, 2021: Status of the fix for vulnerability CVE-2021-45046.
Issue 5 – December 20, 2021: Updated the fix for vulnerability CVE-2021-45046.
Issue 6 – December 21, 2021: Updated the fix for vulnerability CVE-2021-45105.
Issue 7 – January 06, 2022: Status of the fix for vulnerability CVE-2021-44832 and CVE-2021-4104.
Issue 8 – January 06, 2022: Updated the fix for vulnerability CVE-2021-44832 and CVE-2021-4104.

Patch Notes

The information in this section concerns the patch, if any, recommended for Avaya Co-browsing snap-in release 3.8.1.1 in the Resolution above.

Backup before applying the patch

Always, refer to [Avaya Co-Browsing Snap-in Release Notes](#)

Download

For deploying Avaya Co-browsing snap-in 3.8.1.1:

- Go to Avaya Support and enter your Username and Password, then click LOG IN.

2. Mouse over Support by Product at the top of the page and click Downloads in the menu.
3. In the Enter Your Product Here box, enter “Co-Browsing” and select Avaya Co-Browsing Snap-in Release 3.8.x for your installation.
4. Download CoBrowse-svar-3.8.1.1.1330096.svar.

Or download directly from PLDS using download ID CB000000022

Patch install instructions	Service-interrupting?
Please refer to Avaya Co-Browsing Snap-in Release Notes (Chapter 3) for information about deployment	Yes
Verification	
Verify all breeze nodes are updated as per Breeze PSN and corresponding version of Avaya Co-browsing snap-in is deployed.	
Failure	
Contact Avaya Technical support	
Patch uninstall instructions	
Please refer to Avaya Co-Browsing Snap-in Release Notes .	

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.