



## Product Support Notice

© 2021 Avaya Inc. All Rights Reserved.

PSN # PSN005934u

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: 07-Jan-22

Severity/risk level

High

Urgency

Immediately

Name of problem PSN005934u– Avaya Aura Presence Services Log4j2 vulnerabilities

Products affected

[Avaya Aura Presence Services, 7.X,8. X, 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-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](http://support.avaya.com) for updates

Avaya Aura Presence Services Releases 7.X, 8.X and 10.1.0.0 are not vulnerable as it doesn't include log4j jars in the customer artifacts. However, the solution includes Breeze as Presence is deployed in Breeze.

Customers should make sure the Breeze deployed in their Solution address this vulnerability

- Avaya Aura Presence Services Releases 7.X, 8.X and 10.1.0.0 are deployed as snap-ins in Breeze platform.
- Log4j jars used by Avaya Aura Presence Services are part of Breeze platform.

Please refer to Breeze PSN # PSN005949u (<https://download.avaya.com/css/public/documents/101079448>)

### Important Note:

1. **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

Log4j fixes are provided by Breeze platform. Please refer Breeze PSN # PSN005949u

### Workaround or alternative remediation

Not Applicable.

### Remarks

PSN Revision History

Issue 1 – December 15, 2021: Initial publication.

Issue 2 – December 18, 2021: Included CVE-2021-45046 vulnerability in description

Issue 3 – December 21, 2021: Included CVE-2021-45105 vulnerability in description

Issue 4- January 7, 2022: Included CVE-2021-44832, CVE-2021-4104 vulnerability in description

## Patch Notes

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

### 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](http://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](http://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.