



## Product Support Notice

© 2022 Avaya Inc. All Rights Reserved.

PSN # PSN020559u

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

Original publication date: 13

Severity/risk level

High

Urgency

Immediately

-Jan-22. This is issue #01, published date: 13-Jan-22.

Name of problem PSN020559u - Avaya Aura® Communication Manager Log4j vulnerabilities

### Products affected

Avaya Aura® Communication Manager, All 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](http://support.avaya.com) for updates.

- All Communication Manager releases are not impacted by the Log4j 2.x vulnerabilities as Log4j 2.x is not present.
- Communication Manager releases will be flagged on security scans for the presence of Log4j 1.x.
  - Internal analysis has determined that Communication Manager 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 Communication Manager.
  - Internal analysis has determined that Communication Manager releases are not vulnerable to the associated vulnerability CVE-2021-44832 with respect to Log4j 2.x or Log4j 1.x as JndiLookup is not present in the classpath.

This PSN will be updated as more information becomes 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

No action required.

### Workaround or alternative remediation

N/A

### Remarks

PSN Revision History:

Issue 1 – January 13, 2022: Initial publication.

## 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

N/A

### Service-interrupting?

No

### 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.