



## Product Support Notice

© 2021 Avaya Inc. All Rights Reserved.

PSN # PSN005930u

Original publication date: 15-December-2021. This is Issue #4, published date: 4-January- 2022

Severity/risk level

High

Urgency

Immediately

Name of problem

CMS not impacted by Apache Log4j\_2 vulnerabilities.

Products affected

CMS 19.0, CMS 19.1, CMS 19.2

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

This PSN addresses the CMS product only.

No versions of CMS are vulnerable.

CMS is using a version of Log4j that is older than the vulnerable versions and CMS does not use JNDI.

This PSN will be updated as more information is available.

Resolution

n/a

Workaround or alternative remediation

n/a

Remarks

Issue 1 – December 15, 2021: Initial publication.

Issue 2 – December 17, 2021: Updated the fix of vulnerability CVE-2021-44228.

Issue 3 – December 21, 2021: Updated to include information on CVE-2021-45046 and CVE-2021-45105.

Issue 4 – January 4, 2022: Updated to include information on CVE-2021-44832 and CVE-2021-4104.

## Patch Notes

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

Backup before applying the RPM Updates

n/a

Download

n/a

Patch install instructions

n/a

Service-interrupting?

n

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

Not Susceptible

Reference [www.avaya.com/emergencyupdate](http://www.avaya.com/emergencyupdate)

## Mitigation

n/a

**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.