



PSN # PSN005964u

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

Original publication date: 16-Dec-21. This is issue #04, published date: 07-Jan-22.

Severity/risk level

High

Urgency

Immediately

Name of problem PSN005964u – CTSuite Log4j vulnerabilities.

Products affected

CT Suite 3.2, CT Suite 3.3

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

CT Suite Version	Elasticsearch version used	Log4j version	JDK version	Vulnerable to remote code execution	Vulnerable to information leakage	Vulnerable to denial of service	Vulnerable to deserialization of untrusted data
2.5 – 3.1	n/a	n/a	n/a	no	no	no	no
3.2	6.12	2.9.1	8	yes	no	no	no
3.3	6.12, 7.3.x, 7.10.x	2.11.1	8	yes	no	no	no
3.3	7.3.x	2.11.1	12	yes	no	no	no
3.3	6.12, 7.10.x	2.11.1	12	no	no	no	no
4.0	7.11.2 (Elastic cloud)	n/a	n/a	no	no	no	no

Elasticsearch (6.8.9+, 7.8+) used with recent versions of the JDK (JDK9+) is not susceptible to either remote code execution or information leakage. This is due to Elasticsearch’s usage of the Java Security Manager. Most other versions (5.6.11+, 6.4.0+ and 7.0.0+) can be protected via a simple JVM property change. The information leak vulnerability does not permit access to data within the Elasticsearch cluster.

Elasticsearch versions 5.6.11+, 6.4+, and 7.0+ running on JDK8 or below are susceptible to an information leak via DNS which is fixable by following the instructions in the Resolution or Workaround or alternative remediation sections below. The information leak vulnerability does not permit access to data within the Elasticsearch cluster.

Elastic has been updating this announcement below with new details as they emerge from their analysis: Apache Log4j2 Vulnerability - CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 – ESA-2021-31

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

This PSN will be updated as more information is available.

Resolution

Any CT Suite customers on release 3.2 or 3.3 with Elasticsearch version 6.12, 7.3.x, 7.10.x should upgrade Elasticsearch to versions 7.16.2 or 6.8.22 when they are made available from Avaya. These versions will set a JVM property (Dlog4j2.formatMsgNoLookups=true) and remove the vulnerable JndiLookup class from Log4j out of an abundance of caution. This PSN will be updated with the expected release dates. The update will require Avaya services installation. Further details will be provided when the update is made available.

Elasticsearch 7.16.2 and 6.8.22 include Log4j 2.17.0 should not trigger false positives in vulnerability scanners.

Workaround or alternative remediation

Elastic has published an alternative remediation which can be implemented in advance of the new release. If required, the alternative remediation below can be implemented by Avaya services.

If using Elasticsearch (6.8.9+, 7.8+) make sure JDK is (JDK9+) so that you're not susceptible to either remote code execution.

1. [Download the latest version of JDK](#)
2. [Install the latest version of JDK](#)

Elasticsearch version 7.3.x can be protected by applying a simple JVM property change.

Ensure this parameter is configured in the startup scripts of the Java Virtual Machine:

```
-Dlog4j2.formatMsgNoLookups=true
```

[Configure JVM options](#)

Remarks

PSN Revision History

Issue 1 – December 16, 2021: Initial publication.

Issue 2 – December 23, 2021: Update to publication.

Issue 3 – January 03, 2022: Update to publication.

Issue 4 – January 07, 2022: Update to 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

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.