PSN #	PSN005937u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.		
Original publication date: 15-Dec-21. This is issue #06, published date: 01-Feb-22.	Severity/risk level	High	Urgency	Immediately
Name of problem	PSN005937u – Avaya Interaction Center Log4j2 vulnerabilities			

Products affected

Avaya Interaction Center, 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, CVE-2022-23302, CVE-2022-23305, CVE-2022-23307) 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 Interaction Center Release 7.3.9 is impacted by the Log4j2 vulnerabilities CVE-2021-44228, CVE-2021-45105. IC Release 7.3.9 uses log4j v2.13.0 for CSPortal component. As this release uses JDK 8u181, it is vulnerable and may be potentially attacked.

Avaya Interaction Center Release 7.3.10 is impacted by the Log4j2 vulnerabilities CVE-2021-44228, CVE-2021-45105. IC Release 7.3.10 uses log4j v2.13.0 for CSPortal component, but this release also uses JDK 8u292, so it should mitigate CVE-2021-44228, but not CVE-2021-45105.

If you have already upgraded Log4J 2.13 to 2.16.0 or 2.17.0, you must upgrade it once again to 2.17.1 version (see Resolution section) due to CVE-2021-45046 for 2.16.0 or CVE-2021-44832 for 2.17.0 version.

Avaya Interaction Center Releases 7.3.* are running Log4jv1 that are not susceptible.

Internal analysis has determined that IC 7.3.* 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 Interaction Center by default. We recommend checking all log4j.xml files on your IC systems to make sure that this appender has not been added manually.

Internal analysis has determined that IC 7.3.* releases are not vulnerable to the associated vulnerability CVE-2022-23302 (Log4j 1.x JMSSink) although Log4j 1.x is used in the software. This is because JMSSink is not used or configured in any of the log4j configurations for Interaction Center by default. We recommend checking all log4j.xml files on your IC systems to make sure that this appender has not been added manually.

Internal analysis has determined that IC 7.3.* releases are not vulnerable to the associated vulnerability CVE-2022-23305 (Log4j 1.x JDBCAppender) although Log4j 1.x is used in the software. This is because JDBCAppender is not used or configured in any of the log4j configurations for Interaction Center by default. We recommend checking all log4j.xml files on your IC systems to make sure that this appender has not been added manually.

Internal analysis has determined that IC 7.3.* releases are not vulnerable to the associated vulnerability CVE-2022-23307 (Log4j 1.x Chainsaw) although Log4j 1.x is used in the software. This is because Chainsaw is not used or configured in any of the log4j configurations for Interaction Center by default.

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

This PSN will be updated as more information is 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

The patch for CS Portal release versions 7.3.9 and 7.3.10 is available on Avaya Support - Downloads - HF_IC739_IC7310_log4j2_CVE-2021-44228 - Interaction Center. This patch is for CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832.

Workaround or alternative remediation

The actions can be implemented by Customer/Partner.

- For log4j version 1.x (All IC Releases), vulnerable appenders are not configured in OOTB IC packages.

CVE	Mitigation
CVE-2021-4104	Ensure JMSAppender is not used in logging configuration settings. Disable the log4j feature that allows "to load a remote configuration file or to configure the logger through the code".
CVE-2022-23302	- Comment out or remove JMSSink in the Log4j configuration if it is used - Remove the JMSSink class from the server's jar files. For example: zip -q -d log4j-*.jar org/apache/log4j/net/JMSSink.class
CVE-2022-23305	- Comment out or remove JDBCAppender in the Log4j configuration if it is used - Remove the JDBCAppender class from the server's jar files. For example: zip -q -d log4j-*.jar org/apache/log4j/jdbc/JDBCAppender.class
CVE-2022-23307	Avoid using Chainsaw to view logs, and instead use some other utility, especially if there is a log view available within the product itself. - Remove the Chainsaw classes from the log4j jar files. For example: zip -q -d log4j-*.jar org/apache/log4j/chainsaw/*

- For log4j versions 2.10 and later (IC Releases 7.3.9 and 7.3.10):

CVE	Mitigation
CVE-2021-44832	Make sure JDBC Appender is disabled
CVE-2021-44228	Remove the JndiLookup class from the classpath: • zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class.
CVE-2021-45046	Remove the JndiLookup class from the classpath: • zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class.
CVE-2021-45105	Remove **JndiLookup.class** from the classpath: • zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class. **The following mitigation does not fix the issue completely:** • Replace Context Lookups with Thread Context Map Patterns • Remove References to Context Lookups in Pattern Layout in Logging Configuration file Lookups that take place during event processing are still allowed to recurse. The complete fix is to upgrade is to Log4j 2.17.1

Remarks

Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 15, 2021: Added patch info.
Issue 3 – December 17, 2021: Added info related to CVE-2021-45046.
Issue 4 – December 21, 2021: Added info related to CVE-2021-45105, updated *Workaround* section.
Issue 5 – January 3, 2022: Added info related to CVE-2021-44832 and CVE-2021-4104.
Issue 6 – February 1, 2022: Updated *Problem Description* and *Workaround* sections according to new found vulnerabilities CVE-2022-23302, CVE-2022-23305, CVE-2022-23307.

Patch Notes

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

Backup before applying the patch

Always

Download

The patch for CS Portal release versions 7.3.9 and 7.3.10 is available:
Avaya Support - Downloads - HF_IC739_IC7310_log4j2_CVE-2021-44228 - Interaction Center

Patch install instructions — Service-interrupting?

1) Stop CSPortal service. — Yes
2) Backup file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-api-2.x.x.jar and replace this file with the log4j-api-2.17.1.jar file from this patch.
3) Backup file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-core-2.x.x.jar and replace this file with the log4j-core-2.17.1.jar file from this patch.
4) Backup file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-slf4j-impl-2.x.x.jar and replace this file with the log4j-slf4j-impl-2.17.1.jar file from this patch.
5) Start CSPortal server.

Verification

Make sure CSPortal writes logs as earlier

Failure

n/a

Patch uninstall instructions

1) Stop CSPortal server.
2) Restore the backed up file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-api-2.x.x.jar
3) Restore the backed up file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-core-2.x.x.jar
4) Restore the backed up file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-slf4j-impl-2.x.x.jar
5) Start CSPortal server.

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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23302
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23305
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23307

Reference https://logging.apache.org/log4j/2.x/security.html
Reference https://logging.apache.org/log4j/1.2/

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.