PSN #	PSN005976u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.		
Original publication date: 20-Dec-21. This is issue #07, published date: 04-May-22.	Severity/risk level	High	Urgency	Immediately
Name of problem	PSN005976u – Avaya Workforce Engagement Log4j vulnerabilities			
Products affected				
Avaya Workforce Engagement (AWE), 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 Workforce Engagement 15.2 HFR5 and later is impacted by the Log4j2 vulnerability.

Software patch updates are needed in certain components of the Avaya WE 15.2 solution to upgrade the Apache Log4j2 library from 2.x to 2.16.0 to address vulnerabilities CVE-2021-44228 and CVE-2021-45046 as defined in the National Vulnerability Database.

CVE-2021-45105 is susceptible to a DoS attack caused by a Stack-Overflow in Context Lookups in a configuration file's layout patterns. AWE does not use Context Lookups in the AWE 15.2 (HFR5 and later) and above solution, this CVE is not applicable to AWE 15.2 HFR5 and above.

AWE 15.2 HFR5 and above are not vulnerable to the associated vulnerability CVE-2021-44832 (RCE attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server). This is because JDBC Appender is not used in any of the log4j configurations for AWE 15.2 HFR5 and above.

AWE 15.2 HFR5 and above are not vulnerable to the associated vulnerability CVE-2021-4104 (Log4j 1.x JMSAppender) although Log4j 1.x is used in the Avaya Contact Recorder (ACR) software. This is because JMSAppender is not used in any of the log4j configurations for AWE 15.2 HFR5 and above.

Avaya Workforce Engagement 15.2 HFR5 and later has recently identified additional CVE-2022-xxxx assessments below.

AWE 15.2 HFR5 and above is not vulnerable to the associated CVE-2022-23302 (Log4j 1.x JMSSink) although Log4j 1.x is used in the Avaya Contact Recorder (ACR) software. This is dependent on the system being secured as per the documented hardening guidelines. ACR does not leverage this technology.

AWE 15.2 HFR5 and above is not vulnerable to the associated CVE-2022-23325 (Log4j 1.x JDBCAppender) although Log4j 1.x is used in the Avaya Contact Recorder (ACR) software. JDBCAppender is not used in Avaya Workforce Engagement. ACR does not leverage this technology.

AWE 15.2 HFR5 and above is not vulnerable to the associated CVE-2022-23327 ((Log4j 1.x Chainsaw) although Log4j 1.x is used in the Avaya Contact Recorder (ACR) software. Chainsaw is not used in Avaya Workforce Engagement. ACR does not leverage this technology.

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 following table lists the specific software patches (KBs) and kits needed to address the Apache Log4j2 vulnerabilities in **WFE 15.2 HFR7 and higher**. Certain Verint WFE 15.2 solution components require Software patch updates, to upgrade the Apache Log4j2 library from 2.x to 2.17.1. These software updates can be accessed through the Avaya Support portal / PLDS or through the Verint Software Download page in Verint Connect. Customers on WFO Packages 700 through 816 will need to update to WFO 917.

Product Category	Subsystem	PLDS ID	Patch or Kit Number
WFE Suite	Oracle WebLogic	WFO000001066	Security Kit 17 (KB211818)
WFE Suite	WFO Package	WFO000001078	WFO 917 (KB211994)
WFE Suite	Audit Service	WFO000001071	KB211799 or later
Quality Monitoring	AQM Orchestrator	WFO000001067	KB211807 or later
Quality Monitoring	AQM Poller	WFO000001068	KB211883 or later
Quality Monitoring	AQM Scoring Rules Builder	WFO000001069	KB211806 or later
Enterprise Recording	Archiver	WFO000001070	KB211761 or later
Enterprise Recording	Recorder API	WFO000001073	KB211760 or later
Analytics	Speech Categorization x64	WFO000001074	KB211788 or later
Analytics	Transcription Repository Service	WFO000001077	KB211789 or later
Analytics	Text Analytics Application	WFO000001076	KB211906 or later
Customer Feedback	CF ETL	WFO000001072	KB211814 or later
Customer Feedback	Survey Server	WFO000001075	KB211815 or later
Mobile	Mobile Gateway	WFO000001057	KB212036 or later

The following table lists the specific software patches (KBs) and kits needed to address the Apache Log4j2 vulnerabilities in **WFE 15.2 HFR5**. Software patch updates are needed in certain components of the Verint WFE 15.2 solution to upgrade the Apache Log4j2 library from 2.x to 2.16.0. These software updates can be accessed through the Avaya Support portal / PLDS or through the Verint Software Download page in Verint Connect. Customers on WFO Packages HF0700 through HF0816 will need to update to WFO HF0910 or above before applying the KBs for Framework Foundation.

Product Category	Subsystem	PLDS ID	Patch or Kit Number
WFE Suite	Oracle WebLogic	WFO000001041	Security Kit 16b (KB211642)
WFE Suite	Framework Foundation	WFO000001061	KB171899 (for systems on HF0544) or later
WFE Suite	Audit Service	WFO000001046	KB211694 or later
Quality Monitoring	AQM Orchestrator	WFO000001047	KB211698 or later
Quality Monitoring	AQM Poller	WFO000001048	KB211699 or later
Quality Monitoring	AQM Scoring Rules Builder	WFO000001049	KB211697 or later
Enterprise Recording	Archiver	WFO000001050	KB211706 or later
Enterprise Recording	Recorder API	WFO000001051	KB211708 or later
Analytics	Speech Categorization x64	WFO000001052	KB211709 or later
Analytics	Transcription Repository Service	WFO000001053	KB211711 or later
Analytics	Text Analytics Application	WFO000001054	KB211717 or later
Customer Feedback	CF ETL	WFO000001055	KB211710 or later
Customer Feedback	Survey Server	WFO000001056	KB211684 or later
Mobile	Mobile Gateway	WFO000001057	KB202394 or later

Workaround or alternative remediation

N/A

Remarks

PSN Revision History

Issue 1 – December 20, 2021: Initial publication.

Issue 2 – December 22, 2021: Addition of Avaya PLDS details for software downloads. Confirmation that CVE-2021-45105 is not applicable for AWE 15.2 HFR7 and above.

Issue 3 – December 24, 2021: Updated for 15.2 HFR5.
Issue 4 – January 06, 2022: Updated for two further CVEs – both are N/A for AWE.
Issue 5 – January 07, 2022: Title updated.
Issue 6 – February 02, 2022: Updated for three further CVEs (CVE-2202-23302, CVE-2202-23325 and CVE-2202-23327 – all are N/A for AWE.
Issue 7 – May 04, 2022: KB updates to take Log4j to 2.171.1 for 15.2 HFR7 and higher.

Additional Deployment Notes

KB Uninstall Directory Contains Vulnerable Files.

For patch\directory information given below, for Avaya Workforce Engagement installations, the *%IMPACT360SOFTWAREDIR%* directory is *AvayaAura\Software.*

Verint uses the directories in the %IMPACT360SOFTWAREDIR%\hotfixes directory to store previously installed versions of the product. The files in these directories are only used to roll back an installed KB to a previous version.
When a new component (KB) is installed on a Verint server, the existing files (pre-KB install) are backed up to the hotfixes folder.
If the KB is ever rolled back to the previous version, then the backed-up versions from the hotfixes folder will be placed back into the production folders.
When the Hotfix Deployment Fix Tool (HDFT) runs, a process removes entries from the hotfixes folder if the rollback entry is more than 6 months old and the e: drive disk free space is below predetermined thresholds.
If a KB is installed to address a vulnerability in the product, old versions of vulnerable executables are placed in the hotfixes folder. Old versions are kept for the roll back process to work and are not used by the WFE software. If customers wish to remove all copies of the vulnerable files on the server, they can remove any of the KB###### folders. However, removing these folders also removes the ability to uninstall the KBs associated with those rollback folders.

Oracle Weblogic Patch Uninstall Directory Contains Vulnerable Files

Product updates to the Oracle WebLogic component place old Oracle WebLogic patches in the %IMPACT360SOFTWAREDIR%\ProductionServer\.patch_storage directory. Similar to Verint's hotfixes directory, these are used to rollback WebLogic patches if necessary and are not used by the WFE software. Removal of specific patch directories removes the ability to rollback Oracle WebLogic patches.

Oracle WebLogic Update

The following filename that exists on the system may cause confusion:

- %IMPACT360SOFTWAREDIR%\ProductionServer\oracle_common\modules\thirdparty\log4j-2.11.1.jar.

Oracle WebLogic have addressed the vulnerability by upgrading log4j in place. Inspection of the manifest file contents will show that the contents are actually the log4j-core-2.16.0.jar

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://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.