Product Support Notice

PSN #	PSN005931u				
Original publication date: 15-December-2021. This is Issue #06, published date: 11-January-2022.		Severity/risk level	High	Urgency	Immediately
Name of problem	PSN005931u - AACC/ACCS Log4j vulnerabilities.				

Products affected

Avaya Aura® Contact Center (AACC) 7.1.x, Avaya Contact Center Select (ACCS) 7.1.x, Avaya Aura® Contact Center (AACC) 7.0.3, Avaya Contact Center Select (ACCS) 7.0.3

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

AACC 7.1.x, 7.0.3 and ACCS 7.1.x, 7.0.3 are impacted by the Log4j vulnerability (CVE-2021-44228) & (CVE-2021-45046)

AACC 7.1.x, 7.0.3 and ACCS 7.1.x, 7.0.3 are not impacted by the Log4j vulnerabilities (CVE-2021-45105), (CVE-2021-44832) and (CVE-2021-4104)

Resolution

The solutions mentioned in this section address Apache Log4J vulnerability (CVE-2021-44228) and subsequent (CVE-2021-45046) vulnerability

A. Customers on AACC/ACCS 7.1.2

Solution Patches for AACC 7.1.2 are available on https://support.avaya.com/downloads/download-details.action?contentId=1399828504593&productId=P0793&releaseId=7.1.x
Solution Patches for ACCS 7.1.2 are available on https://support.avaya.com/downloads/download-details.action?contentId=1399828503499&productId=P1569&releaseId=7.1.x
AvayaCC_CCCC_7.1.2.0.4.3_Patch.zip
PLDS id: CCTR0000407
AvayaCC_WS_7.1.2.0.5.22_Patch.zip
PLDS id: CCTR0000406

NOTE:

- The CCCC Patch removes the vulnerable JndiLookup class from the log4j 2.8.2 and log4j 2.11.1 core JAR files. The WS Patch upgrades the log4j to version 2.16. If you subsequently scan your AACC/ACCS server it will still flag the log4j JAR files but they are fixed because the JndiLookup class has been removed.
- A log4j 2.8.2 core JAR file exists in the following directory D:\Avaya\Contact Center\CCT\OI_RefClient\lib\cxf\log4j-core-2.8.2.jar, this JAR file is not used by the product and therefore does not make the system vulnerable, if you still have concerns you can run the following command to remove the Jndilookup class "C:\Program Files\7-Zip\7z" d "D:\Avaya\Contact Center\CCT\OI_RefClient\lib\cxf\log4j-core-2.8.2.jar" org/apache/logging/log4j/core/lookup/JndiLookup.class

B. Customers on AACC/ACCS 7.1.1

Solution Patches for AACC 7.1.1 are available on https://support.avaya.com/downloads/download-details.action?contentId=C202010201844239480_8&productId=P0793&releaseId=7.1.x
Solution Patches for ACCS 7.1.1 are available on https://support.avaya.com/downloads/download-details.action?contentId=C202010202112543960_6&productId=P1569&releaseId=7.1.x
AvayaCC_CCCC_7.1.1.0.15.2_Patch.zip
PLDS id: CCTR0000405
AvayaCC_WS_7.1.1.0.35.156_Patch.zip

PLDS id: CCTR0000404

NOTE:

- The CCCC Patch removes the vulnerable JndiLookup class from the log4j 2.8.2 and log4j 2.11.1 core JAR files. The WS Patch upgrades the log4j to version 2.16. If you subsequently scan your AACC/ACCS server it will still flag the log4j JAR files but they are fixed because the JndiLookup class has been removed.
- A log4j 2.8.2 core JAR file exists in the following directory D:\Avaya\Contact Center\CCT\OI_RefClient\lib\cxf\log4j-core-2.8.2.jar, this JAR file is not used by the product and therefore does not make the system vulnerable, if you still have concerns you can run the following command to remove the Jndilookup class "C:\Program Files\7-Zip\7z" d "D:\Avaya\Contact Center\CCT\OI_RefClient\lib\cxf\log4j-core-2.8.2.jar" org/apache/logging/log4j/core/lookup/JndiLookup.class

Workaround or alternative remediation

The solutions mentioned in this section address Apache Log4J vulnerability (CVE-2021-44228) and subsequent (CVE-2021-45046) vulnerability

A. Customers on AACC/ACCS 7.1.0.0 to 7.1.0.3(Non-Workspaces)

Follow these steps to address the vulnerability

1. All AACC services have to be stopped to be able to modify log4j-core-*.jar files
    a. Use System Control and Monitor Utility (SCMU) to stop all AACC services
    b. Stop "CC SMMC Daemon" from Windows Services, this service must be stopped before moving to step c.
    c. Stop "CC SMMC" from Windows Services
2. Use 7-zip utility to remove JndiLookup.class from jars directly
    a. Please run the following command:
    "C:\Program Files\7-Zip\7z" d "D:\Avaya\Contact Center\Common Components\CMF\lib\log4j-core-2.8.2.jar" org/apache/logging/log4j/core/lookup/JndiLookup.class
    b. Please run the following command:
    "C:\Program Files\7-Zip\7z" d "D:\Avaya\Contact Center\Common Components\CMF\lib\cxf\log4j-core-2.11.1.jar" org/apache/logging/log4j/core/lookup/JndiLookup.class
3. Reboot AACC server
4. The procedure has to be applied on MCHA/HA/RGN AACC Servers.

NOTES:

- These steps will remove the vulnerable JndiLookup class from the log4j 2.8.2 and log4j 2.11.1 core JAR files, these steps remove and fix the vulnerability. If you subsequently scan your AACC/ACCS server it will still flag the log4j JAR files but they are fixed because the JndiLookup class has been removed.
- A log4j 2.8.2 core JAR file exists in the following directory D:\Avaya\Contact Center\CCT\OI_RefClient\lib\cxf\log4j-core-2.8.2.jar, this JAR file is not used by the product and therefore does not make the system vulnerable, if you still have concerns you can run the following command to remove the Jndilookup class "C:\Program Files\7-Zip\7z" d "D:\Avaya\Contact Center\CCT\OI_RefClient\lib\cxf\log4j-core-2.8.2.jar" org/apache/logging/log4j/core/lookup/JndiLookup.class

B. Customers on AACC/ACCS 7.1.0.0 to 7.1.0.3(Workspaces)

Upgrade to AACC 7.1.2 and apply the solution patches.

C. Customers on AACC/ACCS 7.0.3.0

Follow these steps to address the vulnerability

1. All AACC services have to be stopped to be able to modify log4j-core-*.jar files
    a. Use System Control and Monitor Utility (SCMU) to stop all AACC services
    b. Stop "CC SMMC Daemon" from Windows Services, this service must be stopped before moving to step c.
    c. Stop "CC SMMC" from Windows Services

2. Use 7-zip utility to remove JndiLookup.class from jars directly
    a. For 7.0.3, please run the following commands:
        - "C:\Program Files\7-Zip\7z" d "D:\Avaya\Contact Center\Common Components\CMF\lib\log4j-core-2.8.2.jar" org/apache/logging/log4j/core/lookup/JndiLookup.class
        - "C:\Program Files\7-Zip\7z" d "D:\Avaya\Contact Center\Common Components\CMF\lib\cxf\log4j-core-2.8.2.jar" org/apache/logging/log4j/core/lookup/JndiLookup.class
3. Reboot AACC server
4. The procedure has to be applied on MCHA/HA/RGN AACC Servers.

NOTE:

- These steps will remove the vulnerable JndiLookup class from the log4j 2.8.2 core JAR file, these steps remove and fix the vulnerability. If you subsequently scan your AACC/ACCS server it will still flag the log4j JAR files but they are fixed because the JndiLookup class has been removed.
- A log4j 2.8.2 core JAR file exists in the following directory D:\Avaya\Contact Center\CCT\OI_RefClient\lib\cxf\log4j-core-2.8.2.jar, this JAR file is not used by the product and therefore does not make the system vulnerable, if you still have concerns you can run the following command to remove the Jndilookup class "C:\Program Files\7-Zip\7z" d "D:\Avaya\Contact Center\CCT\OI_RefClient\lib\cxf\log4j-core-2.8.2.jar" org/apache/logging/log4j/core/lookup/JndiLookup.class

Remarks

Issue 1 – December 15, 2021: Initial publication
Issue 2 – December 15, 2021: Updated date for releasing patches
Issue 3 – December 18, 2021: Added details on the solutions and workarounds
Issue 4 – December 21, 2021: Added info related to CVE-2021-45105.
Issue 5 – December 25, 2021: Updated step.
Issue 6 – January 11, 2022: Updated step.

Patch Notes

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

Backup before applying the patch	
n/a	
Download	
https://support.avaya.com/	
Patch install instructions	**Service-interrupting?**
n/a	Yes
Verification	
n/a	
Failure	
n/a	
Patch uninstall instructions	
Refer to patch readme	

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.