Product Notice #0449

AudioCodes Response to Security Vulnerability
-- Apache Log4j 2 (CVE-2021-44228) --

This Product Notice lists AudioCodes products affected by the recently reported security vulnerability **Apache Log4j 2** (CVE-2021-44228) and provides recommendations to mitigate this security threat.

This vulnerability can be exploited by unauthenticated users to take control of Java-based web servers and launch remote code execution (RCE) attacks. AudioCodes carefully analyzed its products and identified that ARM and SmartTAP 360° make use of the affected Log4j 2 library. Since this vulnerability may pose a severe security risk, AudioCodes will provide software updates that remove this vulnerability and strongly recommends that Customers using the affected products immediately apply the update to protect against this vulnerability.

The table below lists the different product lines and indicates for each whether it is affected by the vulnerability and the availability of a software fix.

Affected Products and Patch Information

Product	Affected	Notes and Patch Availability / Resolution
ARM	Yes	A fix patch is available for ARM Version 9.2 and later. It addresses CVE 2021-45046 and CVE-2021-44228 vulnerabilities for Log4j 2. Customers with ARM versions earlier than 9.2 should first upgrade to ARM Version 9.6 fix1 (ARM 9.6.19 - latest version available on AudioCodes Services Portal), and then continue with the instructions below. ARM SIP Module (SM) is not affected.

Product	Affected	Notes and Patch Availability / Resolution
SmartTAP 360°	Yes	SmartTAP versions earlier than 5.1 are not affected. SmartTAP versions 5.1 and later are affected. SmartTAP will be updated to Log4j 2.16 in the latest security patch for SmartTAP versions 5.1, 5.2, 5.3, and 5.4. To install this security patch, follow the instructions below. AudioCodes' Professional Services will reach out to managed SmartTAP Live Customers to coordinate this security patch update.
OVOC (including Device Manager) **EMS/SEM Version 6.6 and later**	No	Based on the published CVE, the vulnerability is applicable to Log4j 2 (started from JNDI feature introduction in Log4j 2.0 beta). OVOC uses Log4j 1.2.16, for which this feature is not available. Therefore, this vulnerability does not affect OVOC. In addition, the JMSappender service in Log4j is not configured nor used by OVOC/EMS/SEM. However, OVOC will be updated to the latest Log4j 2 during Q1 2022 maintenance release.
Native Teams IP Phones	No	-
Teams Meeting Room Devices	No	-
Generic / UC IP Phones	No	These products don't make use of Log4j.
Hardware and Software-based Session Borders Controllers, VoIP Media Gateways and Multi-Service-Business Routers: - Mediant SBC (including WebRTC Gateway) - Mediant Gateway - Mediant MSBR - MediaPack	No	These products don't make use of Log4j.
Stack Manager	No	This product doesn’t make use of Log4j.
VoiceAI Connect (Enterprise / Cloud)	No	These products don't make use of Log4j.

Product	Affected	Notes and Patch Availability / Resolution
WebRTC SDK / WebRTC Client	No	These products don't make use of Log4j.
CCE	No	This product doesn't make use of Log4j.
CloudBond 365	No	This product doesn't make use of Log4j.
Survivable Branch Appliance (SBA)	No	These products don't make use of Log4j.
User Management Pack 365	No	This product doesn't make use of Log4j.
SIP Phone Support (SPS)	No	This product doesn't make use of Log4j.
Meeting Insights	No	This product doesn't make use of Log4j.
Voca Conversational IVR	No	This product doesn't make use of Log4j.
Fax Server for Microsoft Lync	No	This product doesn't make use of Log4j.
Auto Attendant for Microsoft Lync	No	This product doesn't make use of Java nor Log4j.
Redirect Service	No	This product was updated according to the CVE patch recommendation.

Special Instructions for Installing Patch for ARM

Apply the patch on the ARM Configurator machine. The script automatically distributes itself to all corresponding ARM Routers.

To install the security patch:

1. Download the fix (TAR file) from AudioCodes ShareFile.
2. Copy the downloaded file **CVE_2021_45046_Fix.tar.gz** to the /tmp folder on the Configurator machine:

   ```
   sftp as armAdmin user to /tmp folder
   ```

3. Connect via SSH to the Configurator as **armAdmin** user.
4. Change the user permission:

   ```
   su -
   Password: <password>
   ```

5. Change the directory:

   ```
   cd /tmp
   ```

6. Extract the TAR file:

   ```
   tar xf CVE_2021_45046_Fix.tar.gz -C /tmp/
   ```

7. Run the Python script:

   ```
   ./CVE_2021_45046_Fix.py
   ```

Notes:

- Application downtime is not expected (process is similar to ARM upgrade).
- The proposed sequence of resets (suggested by script) – first Routers, and last Configurator. Please note that if during the procedure one of the Routers is unavailable, the script will not be applied to it.
- Each machine reset (Configurator or Router) takes 2-2.5 minutes.
- If the Router is unavailable or a new Router is added to an existing ARM, the fix can be applied separately using one of the following methods:
  - Run the script again (from Configurator). When prompted to reset each machine, choose **no** for all, except for this specific Router.
  - The TAR file includes a second script called *deleteLookupClass.py*, which can be applied to a specific machine (new ARM or previously unavailable Router). After execution of the script, reset the machine (Router).

Special Instructions for Installing Patch for SmartTAP 360°

Prior to applying the security patch, make sure that PowerShell v4.0 or later is installed on the Windows Server. To check the PowerShell version, run the PowerShell command `$psversiontable.psversion`. If you need to upgrade PowerShell, go to Microsoft's Download Center.

To install the security patch:

1. Download the ZIP file from AudioCodes' ShareFile.
2. Copy the downloaded ZIP package to all servers on which SmartTAP Application Server is deployed.
3. On each server, extract the ZIP package.
4. On each server, execute the following:
   a. Open the command prompt as **Administrator**.
   b. Navigate to the folder containing the patch.
   c. Execute the following command within the patch folder:

      ```
      > ReplaceLog4j.bat
      ```

      For example:

      ```
      d:\Patch\patch_log4j_wrapped>ReplaceLog4j.bat
      ```

   d. When the console's command prompt displays "script finished", verify that the generated log files under **\install_log** are without errors.

Notes:

- Several minutes of application downtime is expected during the installation of the security patch.
- SmartTAP is not affected by CVE-2021-45105, which concerns Apache Log4j 2.17.0 (as SmartTAP logging configuration doesn't use a non-default Pattern Layout with a Context Lookup).