audiocodes

Product Notice #0451

SBC/Media Gateway Software Fixes for Privilege Escalation Vulnerabilities

Two Privilege Escalation vulnerabilities were recently privately reported to AudioCodes. These vulnerabilities allow a privileged Administrator user to gain access to the Session Border Controller (SBC) / Media Gateway underlying Linux OS. Software updates are available to remediate these vulnerabilities for the affected products.

Description of Vulnerabilities

- **Secured Emergency Support Mechanism Vulnerability:**

  AudioCodes devices provide a Secured Emergency Support mechanism that allows AudioCodes support to debug them at the Linux OS level in case of a critical failure. This mechanism is essential to meet strict support SLA obligations. To obtain access to this mechanism, the Customer must provide AudioCodes' Support access to an account on the device with administrative privileges. After this first successful authenticated access to the device, the mechanism requires an additional device-specific password, which is obtained from AudioCodes support and verified by the device. The mechanism to generate this secondary password was compromised, allowing a malicious user with privileged administrative access to the device to generate and obtain such a password.

- **Software Upgrade Mechanism Vulnerability:**

  AudioCodes devices allow a user with security administrative privileges to upgrade the software of the device. Up until now, this upgrade mechanism could be exploited by a malicious user, by loading a malicious file specifically crafted to gain user access to the device's underlying Linux OS.

Affected Products

- **Secured Emergency Support Mechanism Vulnerability:**
  - Mediant VE/SE/CE SBC
  - Mediant 9000/9030/9080 SBC
  - Mediant 4000 SBC
  - Mediant 2600 SBC
  - Mediant 3100 SBC and Media Gateway
  - Mediant 1000 SBC and Media Gateway

  - Mediant 800 SBC, Media Gateway and MSBR
  - Mediant 500 SBC, Media Gateway and MSBR
  - Mediant 500L SBC, Media Gateway and MSBR
  - Mediant 500Li
  - MediaPack 1288
- **Software Upgrade Mechanism Vulnerability:**
  - Mediant VE/SE/CE SBC
  - Mediant 9000/9030/9080 SBC

Resolution

For the **Secured Emergency Support Mechanism** vulnerability, the support-password generation process has been replaced by an advanced mechanism, which prevents it from being hacked.

For the **Software Upgrade Mechanism** vulnerability, software upgrade files (.cmp) of the affected products now verify and prevent the loading of any altered or corrupted files to the device and ensure that only AudioCodes' officially published files are used.

These vulnerabilities have been resolved in the following software versions:

- **SBCs and Media Gateways Version 7.2:** Version 7.20A.258.919 or later
- **SBCs and Media Gateways Version 7.4:** Version 7.40A.250.001 or later
- **MSBRs:** Version 7.24A.356.477 or later

The above versions are available on AudioCodes Services Portal and on Azure and AWS Marketplace.

Important Notes

- Only management accounts with the following privilege levels can exploit these vulnerabilities:
  - Secured Emergency Support Mechanism: Administrator, Security Administrator and Master
  - Software Upgrade Mechanism: Security Administrator and Master
- Customers that are concerned that their devices might be affected by these vulnerabilities are recommended to upgrade them to a version in which they were resolved (see above section).
- Customers must carefully read and follow the upgrade instructions provided in the Release Notes before upgrading their devices.
- Customers are strongly advised to follow AudioCodes existing security guidelines and make sure their privileged users have a strong password.

If you have any questions, contact us at
https://www.audiocodes.com/corporate/offices-worldwide

AudioCodes Ltd. | 1 Hayarden Street | Airport City | Lod | Israel | +972-3-976-4000

Join our mailing list for news and updates