AudioCodes

Product Notice #0229

Shellshock Security Patch for AudioCodes Products

Notice Subject

As part of AudioCodes' policy for communicating newly identified vulnerabilities to security threats, this notice addresses the Shellshock vulnerability by providing a brief description of it and instructions for installing the necessary related AudioCodes' security patches.

Notice Date

November 18, 2014.

Notice Effective Date

Immediate.

Affected Product Family

■ AudioCodes EMS (Element Management System) / SEM (Session Experience Manager) version 6.6 to version 7.0 for installations running Linux CentOS version 5.9 Rev6, and versions 6.2 and 6.6 for installations running Solaris 10.

■ AudioCodes Mediant 8000 and Mediant 5000 Shelf Controllers.

> **Note:** This vulnerability does not impact any other AudioCodes product as these do not include the Bash shell.

AudioCodes Inc.
27 World's Fair Drive, Somerset, NJ 08873
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O. Box 255, Ben Gurion Airport, Israel, 7019900
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/info
Website: www.audiocodes.com

Notice Details

Shellshock (CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, and CVE-2014-6278) is a vulnerability in GNU's Bash shell that gives attackers access to run-remote commands on a vulnerable system.

The vulnerability allows injection of arbitrary commands at a higher privilege (i.e. privilege escalation) in the "shell" (hence the name "shellshock"). In other words, an attacker can issue commands that lead to the complete takeover of the server, if desired.

> ⚠️ **Note:** On all the above affected products, the Bash shell can be accessed and attacked only after user login.

Security Software Patch

> ⚠️ **Note:** The security patches described below will be integrated in a future EMS version 7.0 release.

AudioCodes EMS (Element Management System) / SEM (Session Experience Manager)

Use the instructions below to resolve bash security vulnerability (Linux and Solaris corresponding) on the EMS/SEM products.

- **Linux OS – CentOS 5.9 Rev6:**

  1. Login to the EMS server machine by SSH using acems user (default password is *acems*).
  2. Switch to root user by typing:
     ```
     su – root
     ```
     Default password is *root.*
  3. Download the patch to your PC from the following link:
     https://audiocodes.sharefile.com/d/seb60732907048ab9
  4. Use an FTP client to upload the patch from your PC to the EMS server machine.
  5. On the EMS server machine, enter the following commands:
     ```
     cd ~acems
     tar -xvf UpdateBashLinux.tar
     cd BashUpdate/
     ./UpdateBashLinux.pl
     ```

- **Solaris OS – Solaris 10:**

    1. Login to the EMS server machine by SSH using acems user (default password is *acems*).

    2. Switch to root user by typing:
       ```
       su - root
       ```
       Default password is *root*.

    3. Download the patch to your PC from the following link:
       https://audiocodes.sharefile.com/d/sc84436933a848e28

    4. Use an FTP client to upload the patch from your PC to the EMS server machine.

    5. On the EMS server machine, enter the following commands:
       ```
       cd ~acems
       tar -xvf UpdateBashSolaris.tar
       cd BashUpdate/
       ./UpdateBashSolaris.pl
       ```

AudioCodes Mediant 8000 and Mediant 5000 Shelf Controllers

A patch will be delivered as per customers' request. For more information, contact your AudioCodes representative.