Product Notice #0243

POODLE Security Threat to AudioCodes Products

Notice Subject

As part of AudioCodes' policy for communicating newly identified security threats and vulnerabilities, this notice addresses the POODLE (Padding Oracle On Downgraded Legacy Encryption) threat by providing a brief description of this threat and AudioCodes' planned fix to mitigate it.

Notice Date

April 27, 2015

Notice Effective Date

Immediate

Affected Product Family

- AudioCodes Mediant SBCs and Media Gateways

Notice Details

The POODLE vulnerability allows a man-in-the-middle attacker to decrypt cipher text using a padding oracle side-channel attack. POODLE affects older standards of encryption, specifically Secure Socket Layer (SSL) Version 3. It does not affect the newer encryption mechanism known as Transport Layer Security (TLS). More details are available in the upstream OpenSSL advisory.

Man-in-the-middle attacks require large amounts of time and resources. While the likelihood is low, AudioCodes recommends implementing only TLS to avoid flaws in SSL.

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

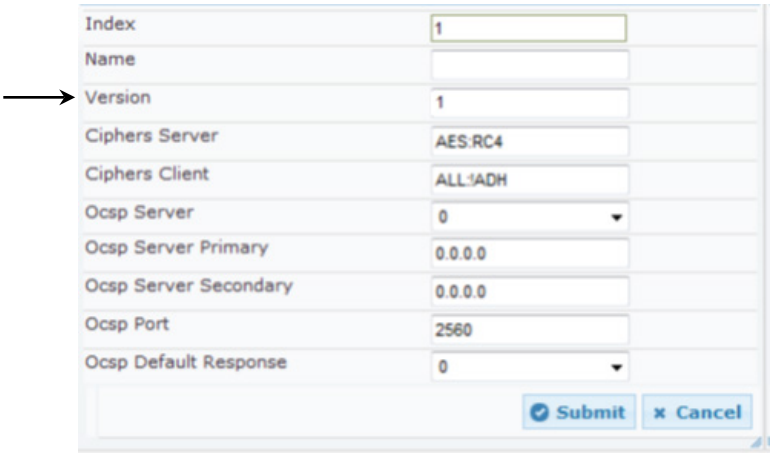
International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O. Box 255, Ben Gurion Airport, Israel, 7019900
Tel: +972-3-976-4000 Fax: +972-3-976-4040

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

Workaround

Version 6.8 and later:

1. Open the TLS Contexts table (**Configuration** tab > **System** menu > **TLS Contexts**).
2. Select a context that you want to configure by selecting its table row, and then clicking **Edit**. The following dialog box appears:



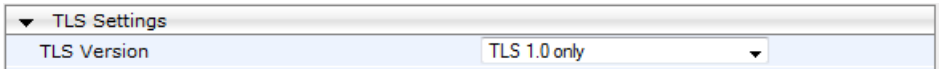
3. Change the 'Version' parameter's value to **1**.

Note: Only TLS 1.0 is used. Clients attempting to connect to the device using any other version are rejected.

4. Click **Submit**, and then save ("burn") your settings to flash memory.
5. Repeat the above steps for all active TLS Contexts.

Version 6.6 and earlier:

1. Open the General Security Settings page (**Configuration** tab > **VoIP** menu > **Security > General Security Settings**).
2. Change the 'TLS Version' parameter's value to **TLS 1.0 Only**.



3. Click **Submit**, and then save ("burn") your settings to flash memory.

Please forward this announcement to relevant customers and partners of AudioCodes.

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