Product Notice #0283

RC4 Encryption No Longer Supported by Web Browsers

Notice Subject

AudioCodes™ calls customers using the Web GUI for device configuration through HTTPS to change the default cipher string (RC4) used by AudioCodes devices.

Notice Date

February 2016

Notice Effective Date

Immediate

Affected Products

All.

Notice Details

RC4 is a stream cipher that has been widely supported across Web browsers for the purpose of encryption. However, since its inception, multiple vulnerabilities have been discovered in RC4 over the years. As a result, the Internet Engineering Task Force (IETF) now (2016) prohibits the use of RC4 with TLS. In addition, Google, Microsoft Edge, Microsoft Internet Explorer, and Mozilla Firefox have announced that they are dropping support for the RC4 cipher in their respective Web browsers.

By default, AudioCodes devices accept only the RC4 cipher string from clients (Web browsers) during the TLS handshake. However, as this cipher string is no longer offered by Web browsers, the device rejects the offered cipher suite (as no match exists) and denies HTTPS access. Therefore, to allow HTTPS access, the list of supported cipher strings must be extended, using the following parameters:

- Global Parameter: **HTTPSCipherString = 'RC4:AES128'**
- TLS Context Table (except MP-1xx and Mediant 2000): **TLSContexts_ServerCipherString = RC4:AES128**

Note: AudioCodes plans to change the default value of these parameters to **RC4:AES128** by the end of Q2 2016.

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