Product Notice #0215

OpenSSL Man-in-the-Middle (MITM) Security Threat to AudioCodes Products

Notice Subject

As part of AudioCodes' policy for communicating newly identified security threats and vulnerabilities, this notice addresses SSL/TLS MITM vulnerability by providing a brief description of this threat and AudioCodes' planned fix to mitigate it.

Notice Date

July 22, 2014

Notice Effective Date

July 22, 2014 or Immediate

Affected Product Family

- AudioCodes' gateways and SBCs with software versions 6.8
- AudioCodes' gateways and SBCs with software versions 6.6

Notice Details

OpenSSL has released a fix for a security flaw (CVE-2014-0224) that is relevant for Man-in-the-middle (MITM) attacks. These attacks potentially allow the attacker to decrypt and modify traffic from the attacked client and server if both are vulnerable.

Note that this vulnerability does not impact AudioCodes IP Phones.

Software Patch

AudioCodes plans to release a software patch to mitigate this security threat for AudioCodes gateways and SBCs with software versions 6.6 and 6.8, no later than **August 26**, **2014**.

In the meantime, AudioCodes **highly recommends** the implementation of TLS mutual authentication to prevent Man in-the-middle (MITM) attacks that are enabled by this security flaw.

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