We change the shape of the world

Security Advisory NTSA2014-01

Issue date: 25th of June 2014

Summary

Several NovaTec products are affected by OpenSSL vulnerability CVE-2014-0224. This may present a vulnerability to MITM attacks, leading to possible information disclosure and modification.

Affected Releases

All NovaTec products incorporating OpenSSL to provide TLS security are affected. Specifically, the following products are vulnerable:

- All Firmware releases up to and including 00.08.02.11 and 00.08.03.01.
- All NMP releases up to and including 7.2.0.4 and 7.3.
- All TI-CA releases up to and including 1.6.0.2.
- All NMS releases up to and including 7.1.2.

No releases of NAMES are affected, as OpenSSL is not used in that product.

Description

Under certain circumstances, where a MITM attack may intercept and alter communication between two affected parties, a “CCS injection” attack (early injection of TLS ChangeCipherSpec command during the handshake) may lead to an apparently secure connection using a zero-length master key. This requires both ends of the connection to be using vulnerable implementations. By altering the TLS handshake and consequently the connection parameters, the MITM can then freely intercept and alter the data transmitted through the TLS connection.

Impact

Should an attacker be able to gain a MITM position between administrative PCs running vulnerable software and vulnerable NovaTec systems, alteration of system configuration and full remote compromise are possible.

Should an attacker be able to gain a MITM position between a vulnerable NovaTec system and a SIP peer, information disclosure and alteration of call flow and routing are possible. This also exposes sRTP keys if sRTP is in use.

Workaround

All NovaTec PC software includes OpenSSL software in the form of DLLs. By replacing these DLLs (ssleay32.dll and libeay32.dll) with compatible versions (32-bit OpenSSL 0.9.8 binaries) without the vulnerability, existing installations may be patched. At the time of writing, 32-bit DLLs for OpenSSL 0.9.8za are freely available on the internet. They may also be taken from installations of non-vulnerable versions of the NovaTec PC tools (see Solutions below).

Other possible workarounds include tunneling traffic through secure VPN connections and ensuring only one end of any connection is vulnerable. This is not a recommended solution and should only be used as a stopgap measure.

Solution

New versions of all NovaTec products address the security vulnerability by including the appropriate fixes. Following versions specifically address CVE-2014-0224:

- Firmware releases 00.08.02.12 and 00.08.03.02.
- NMP releases 7.3.1 and 7.2.0.5.
- TI-CA release 1.6.0.3.

All customers should upgrade to those or later versions.

An update for NMS 7.1.2 is not available, as that product has reached its EOL. Customers still using that product may implement the workaround of replacing the DLLs at their own risk.