6605 19 ½ Mile Road
Sterling Heights, MI 48314-1408 USA
Tel: +586-254-0020, Fax: +586-254-0053
E-mail: security@sisconet.com, Web: http://www.sisconet.com

Security Notice

15 April 2014

Heartbleed Vulnerability Update

On 7 April 2015 US CERT publicly released a notice (http://www.kb.cert.org/vuls/id/720951) that certain versions of the OpenSSL library had a vulnerability (called "Heartbleed") that can be remotely exploited to enable unauthorized access to private encryption keys, and potentially other confidential information, stored on that system. Additional information is available at http://heartbleed.com/ and http://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-099-01B.

The Heartbleed vulnerability only affects V1.0.1 through V1.0.1f of OpenSSL. Other versions of OpenSSL are not affected by Heartbleed.

Impact on SISCO Products

Most existing SISCO products that are installed in operational systems do not use versions of OpenSSL that are vulnerable to Heartbleed. The only SISCO products affected are:

MMS-SECURE-142-064-XXX V11.1
MMS-SECURE-142-095-XXX V11.1

These products are not widely deployed in operational systems at this time. An update to these products will available soon.

NOTE: Many SISCO products that support use of OpenSSL do not embed the OpenSSL library into the SISCO product. On Linux, Solaris and AIX the OpenSSL library is provided by the operating system installation. In those cases the SISCO products dynamically link to the OpenSSL library installed on that computer. Users that are running a SISCO product with the IEC 62351-4 security extensions on a Linux, AIX, or Solaris computing platform will need to verify the OpenSSL version installed on that system and update separately if necessary.

For more information please contact SISCO technical support.