Belden GarrettCom MNS 6K and 10K OpenSSL Vulnerabilities

Date: Aug 09, 2018
Version: 1.0

Summary

The following vulnerabilities affect the OpenSSL library in one or more versions of the Magnum 6K and 10K products listed in the next section:

ID	Title / Description	Severity
CVE-2016-6303	Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.	CVSS v3.0: 9.8
CVE-2016-2182	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.	CVSS v3.0: 9.8
CVE-2016-2177	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.	CVSS v3.0: 9.8
CVE-2016-2176	The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.	CVSS v3.0: 8.2
CVE-2016-0799	The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842.	CVSS v3.0: 9.8
CVE-2016-0705	Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key.	CVSS v3.0: 9.8

Affected Products

Brand	Product Line / Platform	Product	Version
GarrettCom	Magnum Managed Switches	Magnum 6K and 10K	4.7.10 and earlier

Solution

Updates are available that address the vulnerabilities. Customers are advised to update their product to version 4.7.11 or later.

Brand	Product Line / Platform	Product	Version
GarrettCom	Magnum Managed Switches	Magnum 6K and 10K	4.7.11

The OpenSSL Library has been upgraded to the latest version to fix the vulnerabilities in earlier versions of the OpenSSL code.

For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.com and https://garrettcom-support.belden.com.

Disclaimer

Revisions

V1.0 (Aug 09, 2018): Bulletin created.