WEOS-15-07: Security Advisory

CRITICAL / HIGH / **MEDIUM** / LOW 2015-12-04

Description

A security related update of the OpenSSL open source component has been released to fix multiple vulnerabilities, see https://www.openssl.org/news/secadv/20151203.txt. The vulnerabilities have potentially moderate or low impact to Westermo devices. Although the exploitability of WeOS is unknown, WeOS 4.18.0 includes this update.

- Certificate verify crash with missing PSS parameter (CVE-2015-3194)
- X509_ATTRIBUTE memory leak (CVE-2015-3195)
- Race condition handling PSK identify hint (CVE-2015-3196)
  NOTE: Although reported now, it was fixed already in OpenSSL version 1.0.1p, which was included in the WeOS 4.17.1 release

The following of the fixes in the report does not apply to Westermo devices:

- BN_mod_exp may produce incorrect results on x86_64 (CVE-2015-3193)
- Anon DH ServerKeyExchange with 0 p parameter (CVE-2015-1794)

Affected versions

Westermo products running any of the following WeOS operating system versions are potentially susceptible to one or more of the vulnerabilities reported in the OpenSSL update:

4.12.0 and later

Impact

The X.509 certificate based VPN service in WeOS is susceptible to remote denial of service type attacks by using malformed X.509 certificates. Affected services are:

- VPN, virtual private network

Severity

The CVSS[1] severity base score is 6.8.

[1] For more information on CVSS score, see: https://nvd.nist.gov/CVSS-v2-Calculator

Mitigation

We recommend all users with WeOS X.509 certificate based VPN servers to upgrade to WeOS 4.18.0.

Mitigations that do not require update:

- Users that do not use VPN should disable that service. Please consult the Management Guide for more information.

Updates

WeOS version 4.18.0 includes the bundled update from OpenSSL 1.0.1q that fixes all the referred vulnerabilities, and is published on the Westermo download section of the web.

References

https://www.openssl.org/news/secadv/20151203.txt

CVE-2015-3194: OpenSSL: Certificate verify crash with missing PSS parameter

CVE-2015-3195: OpenSSL: X509_ATTRIBUTE memory leak

CVE-2015-3196: Race condition handling PSK identify hint

CVE-2015-3193: BN_mod_exp may produce incorrect results on x86_64

CVE-2015-1794: Anon DH ServerKeyExchange with 0 p parameter