SSA-234763: OpenSSL Vulnerabilities in Siemens Industrial Products

Publication Date: 2014-07-17
Last Update: 2020-02-10
Current Version: V1.6
CVSS v3.1 Base Score: 7.4

SUMMARY

Vulnerabilities in OpenSSL (see https://www.openssl.org/news/secadv_20140605.txt) affect several Siemens industrial products. Siemens has released updates for all affected products.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
APE standalone (only affected if SSL/TLS component is used): All versions < V2.0.2	Update to V2.0.2 http://support.automation.siemens.com/WW/view/en/97654933
CP 1543-1 (incl. SIPLUS NET variants): All versions < V1.1.25	Update to V1.1.25 http://support.automation.siemens.com/WW/view/en/99804563
Crossbow on ROX 2: All versions < V4.2.3	Update to V4.2.3 The firmware update for the Ruggedcom ROX-based devices and ELAN software can be obtained for free either by submitting a support request at http://www.siemens.com/automation/support-request or by calling a local hotline center (see http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx).
ELAN on APE (only affected if SSL/TLS component is used): All versions < V8.4.0	Update to V8.4.0 The firmware update for the Ruggedcom ROX-based devices and ELAN software can be obtained for free either by submitting a support request at http://www.siemens.com/automation/support-request or by calling a local hotline center (see http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx).
ELAN on ROX 2: All versions < V8.4.0	Update to V8.4.0 The firmware update for the Ruggedcom ROX-based devices and ELAN software can be obtained for free either by submitting a support request at http://www.siemens.com/automation/support-request or by calling a local hotline center (see http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx).

ROX 1 (only affected if Crossbow is used): All versions < V1.16.1	Update to V1.16.1 The firmware update for the Ruggedcom ROX-based devices and ELAN software can be obtained for free either by submitting a support request at http://www.siemens.com/automation/support-request or by calling a local hotline center (see http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx).
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V1.6	Update to V1.6 http://support.automation.siemens.com/WW/view/de/98164677
WinCC OA (PVSS): V3.12-P001 - V3.12-P008	Update to 3.12-P009 https://portal.etm.at/index.php?option=com_context&view=category&id=65&layout=blog&Itemid=80

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

RUGGEDCOM APE serves as an utility-grade computing platform for the RUGGEDCOM RX1500 router family. It also allows to run third party software applications without needing to procure an external industrial PC.

The SIMATIC CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

ROX-based VPN endpoints and firewall devices are used to connect devices that operate in harsh environments such as electric utility substations and traffic control cabinets.

Products of the SIMATIC S7-1500 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

The client-server HMI (human machine interface) system SIMATIC WinCC Open Architecture (OA) is part of the SIMATIC HMI family. It is designed for use in applications requiring a high degree of customer-specific adaptability, large or complex applications and projects that impose specific system requirements or functions.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2014-0224

An attacker could perform a man-in-the-middle (MITM) attack between a vulnerable client and a vulnerable server. This vulnerability affects ROX, APE, S7-1500 and CP1543-1.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-310: Cryptographic Issues

Vulnerability CVE-2014-0198

Specially crafted packets may crash the web server of the PLC. This vulnerability affects the SIMATIC S7-1500.

CVSS v3.1 Base Score	5.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-310: Cryptographic Issues

Vulnerability CVE-2014-5298

Specially crafted packets may crash the web server of the PLC. This vulnerability affects the SIMATIC S7-1500.

CVSS v3.1 Base Score	5.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

Vulnerability CVE-2014-3470

Specially crafted packets may crash the web server of the product. This vulnerability affects WinCC OA (PVSS).

CVSS v3.1 Base Score	5.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-310: Cryptographic Issues

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2014-07-17):	Publication Date
V1.1 (2014-08-14):	Added fix for S7-1500
V1.2 (2014-08-21):	Added fix for CP1543-1
V1.3 (2014-10-13):	Added fix for ROX 2 and Crossbow, rearrenged workarounds
V1.4 (2014-10-16):	Added fix for ROX 1
V1.5 (2015-02-13):	Added fix for APE V2.0.2 and ROX V2.6.0 with ELAN
V1.6 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE