SSA-635659: Heartbleed Vulnerability in Siemens Industrial Products

Publication Date:	2014-04-15
Last Update:	2020-02-10
Current Version:	V1.4
CVSS v3.1 Base Score:	7.5

SUMMARY

The “Heartbleed” vulnerability in the OpenSSL cryptographic software library (CVE-2014-0160) affects several Siemens industrial products.

Siemens has resolved the issue in all affected industrial products and provides updates which fix this vulnerability.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
APE: V2.0 when SSL/TLS component is used in customer implementation	Update to V2.0.1 http://support.automation.siemens.com/WW/view/en/97664169
CP 1543-1 (incl. SIPLUS NET variants): V1.1 when FTPS active	Update to V1.1.22 http://support.automation.siemens.com/WW/view/en/92417421
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): V1.5 when HTTPS active	Update to V1.5.1 http://support.automation.siemens.com/WW/view/en/67295862/133100
WinCC OA: V3.12	Update to V3.12-P006 https://portal.etm.at/index.php?option=com_content&view=category&id=65&layout=blo
eLAN-8.2: All versions < V8.3.3 when RIP is used	Update to V8.3.3 The firmware update can be obtained for free by either submitting a support request online (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)

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- WinCC OA: Use VPN for protecting SSL traffic or use WinCC OA in a trusted network
- S7-1500: Disable web server or limit web server access to trusted networks only
- CP1543-1: Disable FTPS, use FTPS in trusted network or use VPN functionality to tunnel FTPS
- APE: Update OpenSSL to 1.0.1g before distributing a solution. Follow instructions from Ruggedcom (see http://support.automation.siemens.com/WW/view/en/97664169) to patch APE 2.0

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

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.

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 SIMATIC CP 1543-1 communication processor 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 such as FTPs. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

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.

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-2014-0160

The affected products could allow attackers to read sensitive data (this includes private keys and user credentials) from the process memory if the attackers have network access to the affected devices.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Joel Langill from Infrastructure Defense Security Services for coordinated disclosure
- 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 (2014-04-15):	Publication Date
V1.1 (2014-04-25):	Added Update Information for WinCC OA V3.12
V1.2 (2014-05-19):	Adjusted CVSS Score for Official Fix, added Update Information for S7-1500 V1.5, CP1543-1 V1.1, and APE2.0
V1.3 (2014-08-14):	New download link for APE
V1.4 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.