SSA-234763: OpenSSL Vulnerabilities in Siemens Industrial Products

Publication Date 2014-07-17
Last Update 2015-02-13
Current Version V1.5
CVSS Overall Score 5.3

Summary:

Vulnerabilities in OpenSSL [1] affect several Siemens industrial products. Siemens has released updates for all affected products.

AFFECTED PRODUCTS

- APE (only affected if SSL/TLS component is used):
  - APE standalone: All versions < V2.0.2
  - ELAN on APE: All versions < V8.4.0
- CP1543-1: All versions < V1.1.25
- ROX 1: All versions < V1.16.1 (only affected if Crossbow is used)
- ROX 2: All versions < V2.6.0 (only affected if ELAN or Crossbow is installed)
  - Crossbow: All versions < V4.2.3
  - ELAN: All versions < V8.4.0
- S7-1500: All versions < V1.6
- WinCC OA (PVSS): V3.12-P001 – V3.12-P008

DESCRIPTION

Vulnerabilities in the OpenSSL cryptographic software library [1] affect several Siemens industrial products. Siemens is working on updates for the affected products and recommends specific countermeasures until fixes are available.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://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.

Vulnerability 1 (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 Base Score 6.8
CVSS Temporal Score 5.3
CVSS Overall Score 5.3 (AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2014-0198)

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

CVSS Base Score	4.3
CVSS Temporal Score	3.2
CVSS Overall Score	3.2 (AV:N/AC:M/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C)

Vulnerability 3 (CVE-2010-5298)

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

CVSS Base Score	4.0
CVSS Temporal Score	3.0
CVSS Overall Score	3.0 (AV:N/AC:H/Au:N/C:N/I:P/A:P/E:U/RL:OF/RC:C)

Vulnerability 4 (CVE-2014-3470)

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

CVSS Base Score	4.3
CVSS Temporal Score	3.4
CVSS Overall Score	3.4 (AV:N/AC:M/Au:N/C:N/I:N/A:P/E:POC/RL:OF/RC:C)

Mitigating factors:

The attacker must have network access to the affected devices. Siemens recommends operating all products except perimeter devices only within trusted networks [7].

SOLUTION

Siemens provides updates for the following products:

- APE V2.0.2 standalone [3][6]
- APE V2.0.2 with ELAN 8.4.0 [3][6]
- CP1543-1 V1.1.25 [5]
- ROX V1.16.1 [6]
- ROX V2.6.0 with Crossbow V4.2.3 [6]
- ROX V2.6.0 with ELAN V8.4.0 [6]
- S7-1500 V1.6 [4]
- WinCC OA (PVSS) 3.12-P009 [2]

Customers can also mitigate the risk of their products by implementing the following steps:

- APE V1.0 with ELAN installed: Follow the Application Note [3]
- Debian with ELAN installed: Update Debian using the standard update procedures

Siemens also recommends protecting network access to all products except for perimeter devices such as CP1543-1 or ROX devices with appropriate mechanisms. It is advised to follow recommended security practices [9] and to configure the environment according to operational guidelines [7] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] Original OpenSSL Security Advisory:
https://www.openssl.org/news/secadv_20140605.txt

[2] The update for WinCC OA can be found on the customer portal (login required):
https://portal.etm.at/index.php?option=com_context&view=category&id=65&layout=blog&Itemid=80

[3] For a fix of APE 1 and APE 2.0, please follow the application note on the Siemens customer service web site:
http://support.automation.siemens.com/WW/view/en/97654933

[4] Firmware version V1.6 for S7-1500 can be obtained here:
http://support.automation.siemens.com/WW/view/de/98164677

[5] Firmware version V1.1.25 for CP1543-1 can be obtained here:
http://support.automation.siemens.com/WW/view/en/99804563

[6] The firmware updates for the Ruggedcom ROX-based devices and ELAN software can be obtained for free from the following contact points:

- Submit a support request online:
http://www.siemens.com/automation/support-request
- Call a local hotline center:
http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx

[7] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf

[8] Information about Industrial Security by Siemens:
http://www.siemens.com/industrialsecurity

[9] Recommended security practices by ICS-CERT:
http://ics-cert.us-cert.gov/content/recommended-practices

[10] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
http://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, rearranged 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

DISCLAIMER