SSA-623229: DROWN Vulnerability in Industrial Products

Publication Date: 2016-04-08
Last Update: 2020-02-10
Current Version: V1.4
CVSS v3.1 Base Score: 4.0

SUMMARY

The disclosed attack called DROWN (Decrypting RSA with Obsolete and Weakened eNcryption), also known as CVE-2016-0800, could potentially allow the decryption of SSL/TLS sessions of some Siemens industrial products under certain conditions.

Siemens has released firmware updates and solutions to resolve the vulnerability

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
ROX I: All versions without solution from SSA-327980	Apply mitigation tool and see SSA-327980 The mitigation tool for the affected ROX I-based products can be obtained by submitting a support request online (https://www.siemens.com/automation/support-request) or by calling a local hotline center (see https://w3.siemens.com/aspa_app/)
SCALANCE X-200 family (incl. SIPLUS NET variants): All versions < V5.2.2	Update to V5.2.2 https://support.industry.siemens.com/cs/ww/de/view/109752018
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions < V5.3.0	Update to V5.3.0 https://support.industry.siemens.com/cs/document/109744096
SCALANCE X-200RNA switch family: All versions < V3.2.5	Update to V3.2.5 https://support.industry.siemens.com/cs/ww/en/view/109745413
SCALANCE X-300 switch family (incl. SIPLUS NET variants): All versions < V4.1.0	Update to V4.1.0 https://support.industry.siemens.com/cs/ww/en/view/109748080
SCALANCE X414: All versions < V3.10.2	Update to V3.10.2 https://support.industry.siemens.com/cs/ww/en/view/109747276

WORKAROUNDS AND MITIGATIONS

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

- Apply appropriate strategies for mitigation.

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

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

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.

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-2016-0800

A cross-protocol attack was discovered that could allow an attacker to decrypt intercepted TLS sessions by using a server supporting SSLv2 as a Bleichenbacher RSA padding oracle. In order to exploit the vulnerability, the attacker must have network access to the affected devices and must be in a privileged network position.

CVSS v3.1 Base Score	4.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

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 (2016-04-08):	Publication Date
V1.1 (2017-02-22):	Update information for SCALANCE X-200 IRT family
V1.2 (2017-06-13):	Update information for SCALANCE X-300 family, X414, X-200 RNA family and ROX I
V1.3 (2017-11-23):	Update information for SCALANCE X-200 family
V1.4 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE