SSA-623229: DROWN Vulnerability in Industrial Products

Publication Date 2016-04-08
Last Update 2017-11-23
Current Version V1.3
CVSSv3 Base Score 4.0

SUMMARY

The disclosed attack called DROWN (Decrypting RSA with Obsolete and Weakened eNcryption), also known as CVE-2016-0800 [1], 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

- SCALANCE X300 family: All versions < V4.1.0
- SCALANCE X414: All versions < V3.10.2
- SCALANCE X200 IRT family: All versions < V5.3.0
- SCALANCE X200 RNA family: All versions < V3.2.5
- SCALANCE X200 family: All versions < V5.2.2
- ROX I: All versions without solution from SSA-327980

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.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3 (CVSSv3) (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 Description (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.

CVSS Base Score 4.0
CVSS Vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

Mitigating Factors

In order to exploit the vulnerability, the attacker must have network access to the affected devices and must be in a privileged network position.

SOLUTION

For SCALANCE X300 family Siemens has released update V4.1.0 [2] and encourages customers apply the update as soon as possible.

For SCALANCE X414 Siemens has released update V3.10.2 [3] and encourages customers apply the update as soon as possible.

For SCALANCE X200 IRT family Siemens has released update V5.3.0 [4] and encourages customers apply the update as soon as possible.

For SCALANCE X200 RNA family Siemens has released update V3.2.5 [5] and encourages customers apply the update as soon as possible.

For ROX I devices Siemens has provided a mitigation tool [6] and application note [7] as part of SSA-327980 [8]. The mitigation tool also disables the use of SSL 2.0 and SSL 3.0 on port 10000/TCP.

For SCALANCE X200 family Siemens has released update V5.2.2 [9] and encourages customers to apply the update as soon as possible.

Siemens has identified the following mitigations that can help to reduce the risk until patches can be applied:

- Protect network access to the web server (443/TCP, 10000/TCP for ROX I by default) on the devices with appropriate mechanisms
- Restrict access to management interface to internal network
- Apply defense-in-depth [10]

As a general security measure Siemens strongly recommends to protect network access to non-perimeter devices with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [10] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] Further information on the DROWN vulnerability:
https://drownattack.com/

[2] Firmware V4.1.0 for SCALANCE X300 family can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109748080

[3] Firmware V3.10.2 for SCALANCE X414 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109747276

[4] Firmware V5.3.0 for SCALANCE X200 IRT family can be obtained from:
https://support.industry.siemens.com/cs/document/109744096

[5] Firmware V3.2.5 for SCALANCE X200 RNA family can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109745413

[6] The mitigation tool for the affected ROX I-based products can be obtained from the following contact points:

- Submit a support request online
  https://www.siemens.com/automation/support-request
- Call a local hotline center:
  https://w3.siemens.com/aspa_app/

[7] The ROX I mitigation tool supporting FAQ (application note) can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109746106

[8] SSA-327980: Vulnerabilities in RUGGEDCOM ROX I can be found here:
https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-327980.pdf

[9] Firmware V5.2.2 for SCALANCE X200 family can be obtained from:
https://support.industry.siemens.com/cs/ww/de/view/109752018

[10] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[11] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[12] For further inquiries on 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 X200 IRT family
V1.2 (2017-06-13):	Update information for SCALANCE X300 family, X414, X200 RNA family and ROX I
V1.3 (2017-11-23):	Update information for SCALANCE X200 family

DISCLAIMER