SSA-102233: SegmentSmack in VxWorks-based Industrial Devices

Publication Date: 2020-04-14
Last Update: 2020-09-08
Current Version: V1.2
CVSS v3.1 Base Score: 7.5

SUMMARY

The latest updates for the affected products fix a vulnerability that could allow remote attackers to affect the availability of the devices under certain conditions.

The underlying TCP stack can be forced to make very computation expensive calls for every incoming packet which can lead to a Denial-of-Service.

Siemens is working on software updates for affected products and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE S602: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE S612: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE S623: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE S627-2M: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-200 switch family (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 443-1 (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 443-1 Advanced (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF180C: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC RF182C: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- For SCALANCE S-600 family (S602, S612, S623, S627-2M): migrate to a successor product within the SCALANCE SC-600 family, V2.1 or later version. For details refer to the notice of discontinuation.
- For SIMATIC RF180C and RF182C: migrate to a successor product within the SIMATIC RF18xC/CI family, V1.3 or later version. For details refer to the notice of discontinuation.
- In all other cases please follow the General Security Recommendations

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

Communication Processor (CP) modules of families SIMATIC NET CP 343-1 and CP 443-1 have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet communication.

Communication Processor (CP) modules SIMATIC NET CP 343-1 Advanced and CP 443-1 Advanced have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet communication.

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

The SCALANCE S-600 devices (S602, S612, S623, S627-2M) are used to protect trusted industrial networks from untrusted networks. The S-600 devices are superseded by the SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C), or the SCALANCE S615.

The SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

SIMATIC RF180C is an RFID communication module for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet. SIMATIC RF180C is superseded by the SIMATIC RF18xC devices (RF185C, RF186C, RF188C).

SIMATIC RF182C is an RFID communication module for direct connection of SIMATIC identification systems to Ethernet/IP. SIMATIC RF182C is superseded by the SIMATIC RF18xC devices (RF185C, RF186C, RF188C).

SIMATIC RF185C, RF186C/CI, and RF188C/CI are communication modules for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet and OPC UA.

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-2019-19301

The VxWorks-based Profinet TCP Stack can be forced to make very expensive calls for every incoming packet which can lead to a denial of service.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

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 (2020-04-14):	Publication Date
V1.1 (2020-08-11):	Added SCALANCE S-600 family and informed about successor products for it
V1.2 (2020-09-08):	Informed about successor products for SIMATIC RF180C and RF182C

TERMS OF USE