SSA-377115: SegmentSmack in Linux IP-Stack 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 has released updates for the affected products and recommends to update to the new versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224: All Versions < V6.1	Update to V6.1 https://support.industry.siemens.com/cs/ww/en/view/109778305/
RUGGEDCOM ROX II: All versions < V2.13.3 only affected by CVE-2018-5391	Update to V2.13.3 https://support.industry.siemens.com/cs/ww/en/view/109778537/
SCALANCE M-800 / S615: All Versions < V6.1	Update to V6.1 https://support.industry.siemens.com/cs/ww/en/view/109778305/
SCALANCE SC-600: All Versions < V2.0	Update to V2.0 or a later version https://support.industry.siemens.com/cs/ww/en/view/109769665/
SCALANCE W1700 IEEE 802.11ac: All Versions < V2.0	Update to V2.0 https://support.industry.siemens.com/cs/ww/en/view/109773734/
SCALANCE W700 IEEE 802.11a/b/g/n: All Versions < V6.4	Update to V6.4 https://support.industry.siemens.com/cs/ww/en/view/109773308/
SIMATIC NET CP 1242-7: All versions < V3.2	Update to V3.2 https://support.industry.siemens.com/cs/ww/en/view/109775640/
SIMATIC NET CP 1243-1 (incl. SIPLUS variants): All versions < V3.2	Update to V3.2 https://support.industry.siemens.com/cs/ww/en/view/109775640/
SIMATIC NET CP 1243-7 LTE EU: All versions < V3.2	Update to V3.2 https://support.industry.siemens.com/cs/ww/en/view/109775640/

SIMATIC NET CP 1243-7 LTE US: All versions < V3.2	Update to V3.2 https://support.industry.siemens.com/cs/ww/en/view/109775640/
SIMATIC NET CP 1243-8 IRC: All versions < V3.2	Update to V3.2 https://support.industry.siemens.com/cs/ww/en/view/109775640/
SIMATIC NET CP 1542SP-1: All versions < V2.1	Update to V2.1 https://support.industry.siemens.com/cs/ww/en/view/109774207/
SIMATIC NET CP 1542SP-1 IRC (incl. SIPLUS variants): All versions < V2.1	Update to V2.1 https://support.industry.siemens.com/cs/ww/en/view/109774207/
SIMATIC NET CP 1543-1 (incl. SIPLUS variants): All versions < V2.2	Update to V2.2 https://support.industry.siemens.com/cs/ww/en/view/109775642/
SIMATIC NET CP 1543SP-1 (incl. SIPLUS variants): All versions < V2.1	Update to V2.1 https://support.industry.siemens.com/cs/ww/en/view/109774207/
SIMATIC RF185C: All versions < V1.3	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109781665
SIMATIC RF186C: All versions < V1.3	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109781665
SIMATIC RF186CI: All versions < V1.3	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109781665
SIMATIC RF188C: All versions < V1.3	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109781665
SIMATIC RF188CI: All versions < V1.3	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109781665
SINEMA Remote Connect Server: All versions >V1.1 and <V2.0.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109777247

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds. Please follow 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

RUGGEDCOM RM1224 is a 4G ROUTER for wireless IP-communication from Ethernet based devices via LTE(4G)- mobile radio, optimized for use in North America.

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.

The SCALANCE M-800 / S615 industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

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.

SCALANCE W1700 products are wireless communication devices used to connect industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs), according to the IEEE 802.11ac standard.

SCALANCE W700 products are wireless communication devices used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

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

The SIMATIC NET CP 1243-1 communication processor connects the S7-1200 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC NET CP 1242-7 and CP 1243-7 LTE communication processors connect the S7-1200 controller to Wide Area Networks (WAN). It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC NET CP 1243-8 IRC communication processor connects S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

The SIMATIC NET CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors 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.

SINEMA Remote Connect ensures management of secure connections (VPN) between headquarters, service technicians and the installed machines or plants.

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-2018-5390

Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() 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:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2018-5391

The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.

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:O/RC:C
CWE	CWE-20: Improper Input Validation

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 (2020-05-12):	Removed IE/PB-Link V3 from affected products
V1.2 (2020-09-08):	Added solution for SIMATIC RF18xC/CI

TERMS OF USE