SSA-462066: Vulnerability known as TCP SACK PANIC in Industrial Products

Publication Date: 2019-09-10
Last Update: 2021-09-14
Current Version: V2.5
CVSS v3.1 Base Score: 7.5

SUMMARY

Multiple industrial products are affected by a vulnerability in the kernel known as TCP SACK PANIC. The vulnerability could allow a remote attacker to cause a denial of service condition.

Siemens has released updates for several affected products and recommends to update to the new versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
CloudConnect 712: All versions < V1.1.5	Update to V1.1.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109769636
ROX II: All versions < V2.13.3 only affected by CVE-2019-11479	Update to V2.13.3 or later version https://support.industry.siemens.com/cs/document/109778537
RUGGEDCOM APE1404 Linux: All versions < Debian 9 Linux Image 2019-12-13 only affected by CVE-2019-11479	Apply the latest available Debian patches https://support.industry.siemens.com/cs/ww/en/view/109773487
RUGGEDCOM RM1224: All versions < V6.2	Update to V6.2 or later version https://support.industry.siemens.com/cs/document/109778305
RUGGEDCOM RX1400 VPE Debian Linux: All versions < Debian 9 Linux Image 2019-12-13 only affected by CVE-2019-11479	Apply the latest available Debian patches in the VPE https://support.industry.siemens.com/cs/ww/en/view/109773485
RUGGEDCOM RX1400 VPE Linux CloudConnect: All versions < Debian 9 Linux Image 2019-12-13 only affected by CVE-2019-11479	Apply the latest available Debian patches in the VPE or apply the latest CloudConnect VPE Linux image https://support.industry.siemens.com/cs/ww/en/view/109773486
SCALANCE M875: All versions	Upgrade hardware to SCALANCE M876-4 or RUGGEDCOM RM1224 and apply patches when available, or follow recommendations from section Workarounds and Mitigations
SCALANCE M-800 / S615: All versions < V6.2	Update to V6.2 or later version https://support.industry.siemens.com/cs/document/109778305

SCALANCE S602: All versions < V4.1 only affected by CVE-2019-8460	Update to V4.1 Update is only available via Siemens Support contact Upgrade hardware to successor product from SCALANCE SC-600 family (https://support.industry.siemens.com/cs/document/109756957) and apply patches when available, or follow recommendations from section Workarounds and Mitigations
SCALANCE S612: All versions < V4.1 only affected by CVE-2019-8460	Update to V4.1 Update is only available via Siemens Support contact Upgrade hardware to successor product from SCALANCE SC-600 family (https://support.industry.siemens.com/cs/document/109756957) and apply patches when available, or follow recommendations from section Workarounds and Mitigations
SCALANCE S623: All versions < V4.1 only affected by CVE-2019-8460	Update to V4.1 Update is only available via Siemens Support contact Upgrade hardware to successor product from SCALANCE SC-600 family (https://support.industry.siemens.com/cs/document/109756957) and apply patches when available, or follow recommendations from section Workarounds and Mitigations
SCALANCE S627-2M: All versions < V4.1 only affected by CVE-2019-8460	Update to V4.1 Update is only available via Siemens Support Contact Upgrade hardware to successor product from SCALANCE SC-600 family (https://support.industry.siemens.com/cs/document/109756957) and apply patches when available, or follow recommendations from section Workarounds and Mitigations
SCALANCE SC-600: All version < V2.0.1	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109769665
SCALANCE W700 IEEE 802.11n: All versions < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109773308
SCALANCE W1700: All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109773734
SCALANCE W1750D: All versions < V8.6.0	Update to V8.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109778052

SCALANCE WLC711: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE WLC712: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CM 1542-1: All versions < 3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109801629/
SIMATIC CP 343-1 Advanced (incl. SIPLUS variants): All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
SIMATIC CP 442-1 RNA: All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 (incl. SIPLUS variants): All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced (incl. SIPLUS variants): All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 OPC UA: All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 RNA: All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
SIMATIC CP 1242-7C: All versions < V3.2	Update to V3.2 or later version https://support.industry.siemens.com/cs/document/109775640
SIMATIC CP 1243-1 (incl. SIPLUS variants): All versions < V3.2	Update to V3.2 or later version https://support.industry.siemens.com/cs/document/109775640
SIMATIC CP 1243-7 LTE EU: All versions < V3.2	Update to V3.2 or later version https://support.industry.siemens.com/cs/document/109775640
SIMATIC CP 1243-7 LTE US: All versions < V3.2	Update to V3.2 or later version https://support.industry.siemens.com/cs/document/109775640
SIMATIC CP 1243-8 IRC: All versions < V3.2	Update to V3.2 or later version https://support.industry.siemens.com/cs/document/109775640
SIMATIC CP 1542SP-1: All versions < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/document/109774207/

SIMATIC CP 1542SP-1 IRC (incl. SIPLUS variants): All versions < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/document/109774207/
SIMATIC CP 1543-1 (incl. SIPLUS variants): All versions < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109775642
SIMATIC CP 1543SP-1 (incl. SIPLUS variants): All versions < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/document/109774207/
SIMATIC CP 1623: All versions < V17.0 only affected by CVE-2019-8460	Update to V17.0 https://support.industry.siemens.com/cs/ww/en/view/109798403
SIMATIC CP 1628: All versions < V17.0 only affected by CVE-2019-8460	Update to V17.0 https://support.industry.siemens.com/cs/ww/en/view/109798403
SIMATIC ITC1500: All versions < V3.1.1.0	Update to V3.1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109783768
SIMATIC ITC1500 PRO: All versions < V3.1.1.0	Update to V3.1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109783768
SIMATIC ITC1900: All versions < V3.1.1.0	Update to V3.1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109783768
SIMATIC ITC1900 PRO: All versions < V3.1.1.0	Update to V3.1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109783768
SIMATIC ITC2200: All versions < V3.1.1.0	Update to V3.1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109783768
SIMATIC ITC2200 PRO: All versions < V3.1.1.0	Update to V3.1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109783768
SIMATIC MV500: All versions < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109781769
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
SIMATIC RF600R: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (MLFB: 6ES7518-4AX00-1AC0, 6AG1518-4AX00-4AC0, incl. SIPLUS variant): All versions < V2.8.4	Update to V2.8.4 https://support.industry.siemens.com/cs/ww/en/view/109761490
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (MLFB: 6ES7518-4FX00-1AC0): All versions < V2.8.4	Update to V2.8.4 https://support.industry.siemens.com/cs/ww/en/view/109761495
SIMATIC Teleservice Adapter IE Advanced: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Teleservice Adapter IE Basic: All versions	See recommendations from section Workarounds and Mitigations
SINEMA Remote Connect Server: All versions < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109777247
SINUMERIK 808D: All versions < V4.92	Update to V4.92 or later version The update can be obtained from your Siemens representative or via Siemens customer service.
SINUMERIK 828D: All versions < V4.8 SP5	Update to V4.8 SP5 or later version The update can be obtained from your Siemens representative or via Siemens customer service.
SINUMERIK 840D sl: All versions < V4.8 SP5	Update to V4.8 SP5 or later version The update can be obtained from your Siemens representative or via Siemens customer service.
TIM 3V-IE (incl. SIPLUS NET variants): All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
TIM 3V-IE Advanced (incl. SIPLUS NET variants): All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
TIM 3V-IE DNP3 (incl. SIPLUS NET variants): All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
TIM 4R-IE (incl. SIPLUS NET variants): All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations

TIM 4R-IE DNP3 (incl. SIPLUS NET variants): All versions only affected by CVE-2019-8460	See recommendations from section Workarounds and Mitigations
TIM 1531 IRC (incl. SIPLUS NET variants): All versions < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109774204

WORKAROUNDS AND MITIGATIONS

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

- Restrict network access to affected devices
- Apply Defense-in-Depth
- For SIMATIC Teleservice Adapters (IE Basic, IE Advanced): migrate to a successor product within the SCALANCE M-800 family. For details refer to the notice of discontinuation.

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

As the virtual machine environment for the RUGGEDCOM RX1400, the RUGGEDCOM VPE1400 is ideally suited for harsh environments, such as those found in electric power, transportation, defense systems and oil and gas industries.

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

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.

RUGGEDCOM APE serves as an utility-grade computing platform for the RUGGEDCOM RX1500 router family. It also allows to run third party software applications without needing to procure an external industrial PC.

SCALANCE W products are wireless communication devices used to connect industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs), according to the IEEE 802.11 standard (802.11ac, 802.11a/b/g/h, and/or 802.11n).

Siemens CloudConnect is used to connect all kinds of plants with the cloud.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

SIMATIC ITC Industrial Thin Clients represent powerful control terminals with high-resolution wide-screen touch displays in 12, 15, 19 and 22 inch formats.

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

SIMATIC RF600 Readers are used for the contactless identification of every kind of object, e.g. transport containers, pallets, production goods, or it can be generally used for recording goods in bulk.

SIMATIC Teleservice adapters allow for remote maintenance of automation systems via phone or internet. The adapters are superseded by the SCALANCE M product family.

SINEMA Remote Connect is a management platform for remote networks that enables the simple management of tunnel connections (VPN) between headquarters, service technicians, and installed machines or plants. It provides both the Remote Connect Server, which is the server application, and the Remote Connect Client, which is an OpenVPN client for optimal connection to SINEMA Remote Connect Server.

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

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.

The SCALANCE M-800 / S615 and RUGGEDCOM RM1224 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 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.

The SCALANCE W1750D controller-based Direct Access Points support radio transmission according to the latest IWLAN standard IEEE 802.11ac Wave 2.

The SIMATIC 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 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 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 CP 1543-1 and SIMATIC CP 1545-1 communication processor 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. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

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

The SIMATIC S7-1500 MFP CPUs provide functionality of standard S7-1500 CPUs with the possibility to run C/C++ Code within the CPU-Runtime for execution of own functions / algorithms implemented in C/C++ and an additional second independent runtime environment to execute C/C++ applications parallel to the STEP 7 program if required.

The stationary optical readers of the SIMATIC MV500 family are used to reliably capture printed, lasered, drilled, punched and dotpeen codes on a variety of different surfaces.

The TIM 3V-IE is a SINAUT ST7 communications module for the SIMATIC S7-300 with an RS232 interface for SINAUT communication via a classic WAN and an RJ45 interface for SINAUT communication via an IP-based network (WAN or LAN).

The TIM 4R-IE DNP3 communication module for SIMATIC S7-300 with an RS232 interface for DNP3 communication via a classic WAN and an RJ45 interface for DNP3 communication via a IP-based network (WAN or LAN).

The TIM 4R-IE is a SINAUT ST7 communications module for the SIMATIC S7-300 with an RS232 interface for SINAUT communication via a classic WAN and an RJ45 interface for SINAUT communication via an IP-based network (WAN or LAN).

TIM 3V-IE advanced communication module for SIMATIC S7-300 with an RS232 interface for SINAUT communication via a classic WAN and an RJ45 interface for SINAUT communication via an IP-based network (WAN or LAN).

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN networks.

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-2019-8460

OpenBSD kernel version <= 6.5 can be forced to create long chains of TCP SACK holes that causes very expensive calls to tcp_sack_option() for every incoming SACK 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-1049: Excessive Data Query Operations in a Large Data Table

Vulnerability CVE-2019-11477

The kernel used in some products is affected by an integer overflow when handling TCP Selective Acknowledgements. A remote attacker could use this to cause 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-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-11478

A remote attacker could cause a denial of service condition by sending specially crafted TCP Selective Acknowledgment (SACK) sequences to affected products.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2019-11479

An attacker with network access to affected products could cause a denial of service condition because of a vulnerability in the TCP retransmission queue implementation kernel when handling TCP Selective Acknowledgements (SACK).

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

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 (2019-09-10):	Publication Date
V1.1 (2019-10-08):	Added solution for SINUMERIK 840D sl, SINUMERIK 828D, SINUMERIK 808D
V1.2 (2019-11-12):	Added solution for SIMATIC MV500. Removed SIMATIC RF166C from affected products
V1.3 (2019-12-10):	Added solution for SCALANCE W700. SIPLUS devices now explicitly mentioned in the list of affected products
V1.4 (2020-02-11):	Added solution for TIM 1531 IRC, for SIMATIC NET CP 1242-7, CP 1243-7 LTE (EU and US versions), CP 1243-1, CP 1243-8 IRC, CP 1543-1, CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1 and for SCALANCE W1700. Added products RUGGEDCOM APE1404 and RUGGEDCOM RX1400. Information regarding SINEMA Remote Connect Server corrected
V1.5 (2020-03-10):	Added solution for SINEMA Remote Connect Server, SCALANCE M-800 / S615 and RUGGEDCOM RM1224. Added products SIMATIC NET CP 1623 and CP 1628. Information regarding SIMATIC MV500 corrected
V1.6 (2020-04-14):	Added solution for ROX II
V1.7 (2020-06-09):	Added products SIMATIC NET CP 443-1 OPC UA, CP 443-1 RNA, CP 442-1 RNA, CP 443-1, CP 443-1 Advanced and CP 343-1 Advanced. Included additional information to CP 1623 and CP 1628 regarding affected CVE. Added CVE-2019-8460 - affected products are identified accordingly.
V1.8 (2020-08-11):	Informed about successor product for SIMATIC Teleservice adapters
V1.9 (2020-09-08):	Added solution for SIMATIC RF18xC/CI
V2.0 (2020-10-13):	Added solution for SIMATIC MV500 and SCALANCE W1750D
V2.1 (2020-12-08):	Added solution for SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP
V2.2 (2021-04-13):	Added affected products SCALANCE S602, SCALANCE S612, SCALANCE S623, and SCALANCE S627-2M and added solution for SIMATIC ITC1500 (PRO), SIMATIC ITC1900 (PRO), and SIMATIC ITC2200 (PRO)
V2.3 (2021-05-11):	Added affected products TIM 3V-IE, TIM 3V-IE Advanced, TIM 3V-IE DNP3, TIM 4R-IE and TIM 4R-IE DNP3
V2.4 (2021-07-13):	Added solution for SIMATIC NET CP 1623 and SIMATIC NET CP 1628
V2.5 (2021-09-14):	Added solution for SIMATIC NET CM 1542-1

TERMS OF USE