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

Publication Date: 2019-09-10
Last Update: 2019-09-10
Current Version: V1.0
CVSS v3.0 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 that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until updates are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
CM 1542-1: All versions	See recommendations from section Workarounds and Mitigations
CP 1242-7: All versions	See recommendations from section Workarounds and Mitigations
CP 1243-1: All versions	See recommendations from section Workarounds and Mitigations
CP 1243-7 LTE EU: All versions	See recommendations from section Workarounds and Mitigations
CP 1243-7 LTE US: All versions	See recommendations from section Workarounds and Mitigations
CP 1243-8 IRC: All versions	See recommendations from section Workarounds and Mitigations
CP 1542SP-1: All versions	See recommendations from section Workarounds and Mitigations
CP 1542SP-1 IRC: All versions	See recommendations from section Workarounds and Mitigations
CP 1543-1: All versions	See recommendations from section Workarounds and Mitigations
CP 1543SP-1: All versions	See recommendations from section Workarounds and Mitigations

CloudConnect 712: All versions < V1.1.5	Update to V1.1.5 https://support.industry.siemens.com/cs/ww/en/view/109769636
ROX II: All versions only affected by CVE-2019-11479	See recommendations from section Workarounds and Mitigations
RUGGEDCOM RM1224: All versions	See recommendations from section Workarounds and Mitigations
S7-1500 CPU 1518(F)-4 PN/DP MFP: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE M800: All versions	See recommendations from section Workarounds and Mitigations
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 S615: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE SC-600: All version < V2.0.1	Update to V2.0.1 https://support.industry.siemens.com/cs/ww/en/view/109769665
SCALANCE W-700 (IEEE 802.11n): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE W1700: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE WLC711: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE WLC712: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC1500: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC1500 PRO: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC1900: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC1900 PRO: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC2200: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC ITC2200 PRO: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC MV500: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF166C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF185C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF186C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF186CI: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF188C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF188CI: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF600R: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Teleserver Adapter IE Advanced: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Teleserver Adapter IE Basic: All versions	See recommendations from section Workarounds and Mitigations
SINEMA Remote Connect Server: All versions < V2.0 SP1	Update to V2.0 SP1 https://support.industry.siemens.com/cs/ww/en/view/109770899
SINUMERIK 808D: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK 828D: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK 840D sl: All versions	See recommendations from section Workarounds and Mitigations
TIM 1531 IRC: 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:

- Restrict network access to affected devices
- Apply Defense-in-Depth

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

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 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 firewall is used to protect trusted industrial networks from untrusted networks. It allows filtering incoming and outgoing network connections in different ways.

The SCALANCE SC firewall is used to protect trusted industrial networks from untrusted networks. It allows filtering incoming and outgoing network connections in different ways.

SCALANCE W-700 products are wireless communication devices which offer reliability, ruggedness and security for both non-critical communication and process-critical data. The devices are used where mobility of machines and parts is required, or cable installation is too expensive or difficult to implement.

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

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.

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7 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.

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

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.

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

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

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.

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 Teleservice allows for remote maintenance of automation systems via phone or internet.

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, 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.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

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 v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

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 v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

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 v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

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

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.