SSA-480230: Denial-of-Service in Webserver of Industrial Products

Publication Date: 2019-04-09
Last Update: 2019-05-14
Current Version: V1.1
CVSS v3.0 Base Score: 7.5

SUMMARY

A vulnerability in the affected devices could allow an unauthorized attacker with network access to the webserver of an affected device to perform a denial-of-service attack.

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 patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
CP1604: All versions	See recommendations from section Workarounds and Mitigations
CP1616: All versions	See recommendations from section Workarounds and Mitigations
SIAMTIC RF185C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP343-1 Advanced: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP443-1: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP443-1 Advanced: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP443-1 OPC UA: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200 SP Open Controller CPU 1515SP PC: All versions < V2.1.6	Update to V2.1.6 https://support.industry.siemens.com/cs/ww/de/view/109759122
SIMATIC ET 200 SP Open Controller CPU 1515SP PC2: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort Outdoor Panels 7" & 15": All versions	See recommendations from section Workarounds and Mitigations

SIMATIC HMI Comfort Panels 4" - 22": All versions	See recommendations from section Workarounds and Mitigations
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 und KTP900F: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC DiagMonitor: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF181-EIP: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF182C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF186C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF188C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF600R: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family: All versions < V2.6.1	Update to V2.6.1 https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 Software Controller: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU family: All versions < V3.X.16	Update to V3.X.16 https://support.industry.siemens.com/cs/ww/en/ps/13752/dl
SIMATIC S7-400 PN (incl. F) V6 and below: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V7 (incl. F): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions < V2.0 SP1 UPD1	Update to V2.0 SP1 UPD1 https://support.industry.siemens.com/cs/de/de/view/109764222
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
SIMATIC Teleservice Adapter IE Standard: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX 2010: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC WinCC Runtime Advanced: All versions	See recommendations from section Workarounds and Mitigations
SIMOCODE pro V EIP: All versions	See recommendations from section Workarounds and Mitigations
SIMOCODE pro V PN: All versions	See recommendations from section Workarounds and Mitigations
SINAMICS G130 V4.6 (Control Unit): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109764679/
SINAMICS G130 V4.7 (Control Unit): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109764679/
SINAMICS G130 V4.7 SP1 (Control Unit): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109764679/
SINAMICS G130 V4.8 (Control Unit): All versions < V4.8 HF6	Update to V4.8 HF6 https://support.industry.siemens.com/cs/ww/en/view/109742040
SINAMICS G130 V5.1 (Control Unit): All versions	See recommendations from section Workarounds and Mitigations
SINAMICS G130 V5.1 SP1 (Control Unit): All versions < V5.1 SP1 HF4	Update to V5.1 SP1 HF4 https://support.industry.siemens.com/cs/ww/en/view/109765015
SINAMICS G150 V4.6 (Control Unit): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109764679/
SINAMICS G150 V4.7 (Control Unit): All versions	See recommendations from section Workarounds and Mitigations
SINAMICS G150 V4.7 SP1 (Control Unit): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109764679/
SINAMICS G150 V4.8 (Control Unit): All versions < V4.8 HF6	Update to V4.8 HF6 https://support.industry.siemens.com/cs/ww/en/view/109742040
SINAMICS G150 V5.1 (Control Unit): All versions	See recommendations from section Workarounds and Mitigations
SINAMICS G150 V5.1 SP1 (Control Unit): All versions < V5.1 SP1 HF4	Update to V5.1 SP1 HF4 https://support.industry.siemens.com/cs/ww/en/view/109765015
SINAMICS S120 V4.6 (Control Unit): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109762626
SINAMICS S120 V4.7 (Control Unit): All versions	See recommendations from section Workarounds and Mitigations

SINAMICS S120 V4.7 SP1 (Control Unit): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109762626
SINAMICS S120 V4.8 (Control Unit): All versions < V4.8 HF6	Update to V4.8 HF6 https://support.industry.siemens.com/cs/ww/en/view/109740193
SINAMICS S120 V5.1 (Control Unit): All versions	See recommendations from section Workarounds and Mitigations
SINAMICS S120 V5.1 SP1 (Control Unit): All versions < V5.1 SP1 HF4	Update to V5.1 SP1 HF4 https://support.industry.siemens.com/cs/ww/en/view/109758423
SINAMICS S150 V4.6 (Control Unit): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109764679/
SINAMICS S150 V4.7 (Control Unit): All versions	See recommendations from section Workarounds and Mitigations
SINAMICS S150 V4.7 SP1 (Control Unit): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109764679/
SINAMICS S150 V4.8 (Control Unit): All versions < V4.8 HF6	Update to V4.8 HF6 https://support.industry.siemens.com/cs/ww/en/view/109742040
SINAMICS S150 V5.1 (Control Unit): All versions	See recommendations from section Workarounds and Mitigations
SINAMICS S150 V5.1 SP1 (Control Unit): All versions < V5.1 SP1 HF4	Update to V5.1 SP1 HF4 https://support.industry.siemens.com/cs/ww/en/view/109765015
SINAMICS S210 V5.1 (Control Unit): All versions	See recommendations from section Workarounds and Mitigations
SINAMICS S210 V5.1 SP1 (Control Unit): All versions	See recommendations from section Workarounds and Mitigations
SITOP Manager: All versions	See recommendations from section Workarounds and Mitigations
SITOP PSU8600: All versions	See recommendations from section Workarounds and Mitigations
SITOP UPS1600: 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:

- Apply appropriate strategies for mitigation as described in the general security recommendation section.
- Restrict network access to the integrated webserver.
- Deactivate the webserver if not required, and if deactivation is supported by the product.
- For SINAMICS S, G130, G150 devices: perform upgrade to a new fixed version, for example version V5.2.

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), 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

Siemens SIMATIC S7-300 CPU families, S7-400 CPU families, S7-1200 CPU families, and S7-1500 CPU families have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

SIMATIC S7-PLCSIM Advanced enables you to create virtual controllers for simulating S7-1500 and ET 200SP controllers and provides extensive simulation of functions.

The SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

SIMATIC WinAC RTX is a SIMATIC software controller for PC-based automation solutions.

CP 1616 and CP 1604 are PCI/PCI-104 cards for high-performance connection of field devices to Industrial Ethernet with PROFINET.

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.

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.

The SITOP PSU8600 expandable power supply system is connected to a 3-phase AC line supply to offer regulated DC power.

SITOP UPS1600 devices augment DC 24V power supply units to offer uninterruptible rated currents up to 40A from battery modules.

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

The SINAMICS converter family is used to control a wide variety of drives, especially in mechanical engineering and plant construction.

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

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

SIMATIC RF182C is a RFID communication module for Ethernet TCP/IP and XML to connect two serial SIMAITC identification readers to a PC or another programmable device able to communicate via Ethernet TCP/IP and XML.

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-2019-6568

The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service condition. An attacker may cause a denial-of-service situation which leads to a restart of the webserver of the affected device.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

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

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 (2019-04-09):	Publication Date
V1.1 (2019-05-14):	Specification for SINAMICS products, added solution for SIMATIC S7-1500 CPU family and SIMATIC S7-PLCSIM Advanced

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.