

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

Publication Date: 2019-04-09
 Last Update: 2020-09-08
 Current Version: V2.0
 CVSS v3.1 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 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
RFID 181EIP: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions < V2.1.6	Update to V2.1.6 https://support.industry.siemens.com/cs/ww/de/view/109759122
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V2.7	Update to V2.7 https://support.industry.siemens.com/cs/ww/en/view/109759122
SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants): All versions < V15.1 Upd 4	Update to V15.1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109763890
SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants): All versions < V15.1 Upd 4	Update to V15.1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109763890
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F: All versions < V15.1 Upd 4	Update to V15.1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109763890
SIMATIC IPC DiagMonitor: All versions < V5.1.3	Update to V5.1.3 https://support.industry.siemens.com/cs/ww/en/view/109763202
SIMATIC NET CP 1616 and CP 1604: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 343-1 Advanced (incl. SIPLUS 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 NET CP 443-1 OPC UA: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF182C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF185C: All versions < V1.1.0	Update to V1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109768507
SIMATIC RF186C: All versions < V1.1.0	Update to V1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109768507
SIMATIC RF188C: All versions < V1.1.0	Update to V1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109768507
SIMATIC RF600 family: All versions < V3.2.1	Update to V3.2.1 https://support.industry.siemens.com/cs/ww/en/view/109768501
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): 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 < V2.7	Update to V2.7 https://support.industry.siemens.com/cs/ww/en/view/109478528
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): 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/DP V6 and below CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): 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 (F) 2010: All versions < SIMATIC WinAC RTX 2010 SP3	Update to SIMATIC WinAC RTX 2010 SP3 and apply BIOS and Microsoft Windows updates https://support.industry.siemens.com/cs/ww/en/view/109765109
SIMATIC WinCC Runtime Advanced: All versions < V15.1 Upd 4	Update to V15.1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109763891
SIMOCODE pro V EIP (incl. SIPLUS variants): All versions < V1.1.3	Update to V1.1.3 https://support.industry.siemens.com/cs/ww/en/view/109756912
SIMOCODE pro V PN (incl. SIPLUS variants): All versions < V2.1.3	Update to V2.1.3 https://support.industry.siemens.com/cs/ww/en/view/109749989
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	Update to V5.1 SP1 HF4 or later version, or to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109765015
SINAMICS G130 V5.1 SP1 Control Unit: All versions < V5.1 SP1 HF4	Update to V5.1 SP1 HF4 or later version 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	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109764679/
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	Update to V5.1 SP1 HF4 or later version, or to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109765015
SINAMICS G150 V5.1 SP1 Control Unit: All versions < V5.1 SP1 HF4	Update to V5.1 SP1 HF4 or later version https://support.industry.siemens.com/cs/ww/en/view/109765015
SINAMICS S120 V4.6 Control Unit (incl. SIPLUS variants): 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 (incl. SIPLUS variants): All versions	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109762626
SINAMICS S120 V4.7 SP1 Control Unit (incl. SIPLUS variants): 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 (incl. SIPLUS variants): 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 (incl. SIPLUS variants): All versions	Update to V5.1 SP1 HF4 or later version, or to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109758423
SINAMICS S120 V5.1 SP1 Control Unit (incl. SIPLUS variants): All versions < V5.1 SP1 HF4	Update to V5.1 SP1 HF4 or later version 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	Update to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109764679/
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	Update to V5.1 SP1 HF4 or later version, or to latest version of V5.2 https://support.industry.siemens.com/cs/ww/en/view/109765015
SINAMICS S150 V5.1 SP1 Control Unit: All versions < V5.1 SP1 HF4	Update to V5.1 SP1 HF4 or later version 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 < V1.1	Update to V1.1 https://support.industry.siemens.com/cs/ww/en/view/109760607
SITOP PSU8600: All versions < V1.5	Update to V1.5 https://support.industry.siemens.com/cs/ww/en/view/102295547
SITOP UPS1600 (incl. SIPLUS variants): All versions < V2.3	Update to V2.3 https://support.industry.siemens.com/cs/ww/en/view/79207181
TIM 1531 IRC (incl. SIPLUS NET variants): All versions < V2.1	Update to V2.1 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:

- 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 SIMATIC Teleservice Adapters (IE Basic, IE Standard, IE Advanced): migrate to a successor product within the SCALANCE M-800 family. 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](#).

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

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 (F) 2010 is a SIMATIC software controller for PC-based automation solutions.

SIMATIC NET 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, 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.

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.

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.

SITOP Manager is a tool for commissioning, engineering and monitoring of SITOP power supplies with communication capabilities.

SIMATIC IPC DiagMonitor monitors, reports, visualizes and logs the system states of the SIMATIC IPCs. It communicates with other systems and reacts when events occur.

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

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.

RFID 181EIP is an RFID communication module for direct connection of SIMATIC identification systems to Ethernet/IP. RFID 181EIP 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.

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).

SIMOCODE is the flexible and modular motor management system for low-voltage motors.

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.

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-2019-6568

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 v3.1 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-125: Out-of-bounds Read

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 (2019-04-09):	Publication Date
V1.1 (2019-05-14):	Specification for SINAMICS products, added solution for SIMATIC S7-1500 CPU family and SIMATIC S7-PLCSIM Advanced
V1.2 (2019-06-11):	Added update for SIMATIC Software Controller and SIMATIC ET 200 SP Open Controller CPU 1515SP PC2
V1.3 (2019-07-09):	Added update for SIMATIC RF600 family, SIMATIC RF185C, SIMATIC RF186C, and SIMATIC RF188C
V1.4 (2019-10-08):	Renamed SIMATIC WinAC RTX 2010 to SIMATIC WinAC RTX (F) 2010 and added update for SIMATIC WinAC RTX (F) 2010
V1.5 (2020-01-14):	Added update for WinCC Runtime Advanced, SITOP Manager, SITOP UPS1600, and SIMATIC HMI Panels. SIPLUS devices now explicitly mentioned in the list of affected products
V1.6 (2020-02-11):	Added update for SITOP PSU8600, TIM 1531 IRC
V1.7 (2020-03-10):	Added update for SIMATIC IPC DiagMonitor
V1.8 (2020-06-09):	Added update for SIMOCODE pro V PN; clarified update version information for SINAMICS G130/G150/S150 and SINAMICS S120
V1.9 (2020-08-11):	Added update for SIMOCODE pro V EIP; informed about successor product for SIMATIC Teleservice adapters
V2.0 (2020-09-08):	Informed about successor products for SIMATIC RF180C and RFID 181EIP

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.