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

Publication Date: 2019-04-09
Last Update: 2023-05-09
Current Version: V2.7
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 latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 (6GK7443-1EX30-0XE0): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 (6GK7443-1EX30-0XE1): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 OPC UA (6GK7443-1UX00-0XE0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1604 (6GK1160-4AA01): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1616 (6GK1161-6AA02): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC ET 200pro IM154-8 PN/DP CPU (6ES7154-8AB01-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/47354502/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM154-8F PN/DP CPU (6ES7154-8FB01-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/47354578/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM154-8FX PN/DP CPU (6ES7154-8FX00-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/62612377/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200S IM151-8 PN/DP CPU (6ES7151-8AB01-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/47353723/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200S IM151-8F PN/DP CPU (6ES7151-8FB01-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/47354354/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V2.7	Update to V2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/ See further 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 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/ See further recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants): All versions < V15.1 Upd4	Update to V15.1 Upd4 or later version https://support.industry.siemens.com/cs/ww/en/view/109763890/ See further recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants): All versions < V15.1 Upd4	Update to V15.1 Upd4 or later version https://support.industry.siemens.com/cs/ww/en/view/109763890/ See further recommendations from section Workarounds and Mitigations
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F: All versions < V15.1 Upd4	Update to V15.1 Upd4 or later version https://support.industry.siemens.com/cs/ww/en/view/109763890/ See further recommendations from section Workarounds and Mitigations

SIMATIC IPC DiagMonitor: All versions < V5.1.3	Update to V5.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109763202/ See further recommendations from section Workarounds and Mitigations
SIMATIC RF182C (6GT2002-0JD10): All versions	Currently no fix is planned Migrate to a successor product within the SIMATIC RF18xC/CI family, V1.3 (see https://support.industry.siemens.com/cs/ww/en/view/109781665) or later version. For details refer to the phase-out announcement at https://support.industry.siemens.com/cs/ww/en/view/109783832 See further recommendations from section Workarounds and Mitigations
SIMATIC RF185C (6GT2002-0JE10): All versions < V1.1.0	Update to V1.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109768507/ See further recommendations from section Workarounds and Mitigations
SIMATIC RF186C (6GT2002-0JE20): All versions < V1.1.0	Update to V1.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109768507/ See further recommendations from section Workarounds and Mitigations
SIMATIC RF188C (6GT2002-0JE40): All versions < V1.1.0	Update to V1.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109768507/ See further recommendations from section Workarounds and Mitigations
SIMATIC RF600R family: All versions < V3.2.1	Update to V3.2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109768501/ See further recommendations from section Workarounds and Mitigations
SIMATIC RFID 181EIP (6GT2002-0JD20): All versions	Currently no fix is planned Migrate to a successor product within the SIMATIC RF18xC/CI family, V1.3 (see https://support.industry.siemens.com/cs/ww/en/view/109781665) or later version. For details refer to the phase-out announcement at https://support.industry.siemens.com/cs/ww/en/view/109783832 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 314C-2 PN/DP (6ES7314-6EH04-0AB0): All versions < V3.3.16	Update to V3.3.16 or later version https://support.industry.siemens.com/cs/ww/en/view/51466769/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EH14-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/40360647/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315F-2 PN/DP (6ES7315-2FJ14-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/40944925/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315T-3 PN/DP (6ES7315-7TJ10-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/85049260/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317-2 PN/DP (6ES7317-2EK14-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/40362228/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317F-2 PN/DP (6ES7317-2FK14-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/40945128/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317T-3 PN/DP (6ES7317-7TK10-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/85059804/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317TF-3 PN/DP (6ES7317-7UL10-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/85063017/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 319-3 PN/DP (6ES7318-3EL01-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/44442927/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 319F-3 PN/DP (6ES7318-3FL01-0AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/44443101/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.6.1	Update to V2.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions < V2.7	Update to V2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478528/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions < V2.0 SP1 UPD1	Update to V2.0 SP1 UPD1 or later version https://support.industry.siemens.com/cs/ww/en/view/109764222/ See further recommendations from section Workarounds and Mitigations
SIMATIC Teleservice Adapter IE Advanced: All versions	Currently no fix is planned Migrate to a successor product within the SCALANCE M-800 family. For details refer to the notice of discontinuation at https://support.industry.siemens.com/cs/ww/en/view/109781070 See further recommendations from section Workarounds and Mitigations
SIMATIC Teleservice Adapter IE Basic: All versions	Currently no fix is planned Migrate to a successor product within the SCALANCE M-800 family. For details refer to the notice of discontinuation at https://support.industry.siemens.com/cs/ww/en/view/109781070 See further recommendations from section Workarounds and Mitigations
SIMATIC Teleservice Adapter IE Standard: All versions	Currently no fix is planned Migrate to a successor product within the SCALANCE M-800 family. For details refer to the notice of discontinuation at https://support.industry.siemens.com/cs/ww/en/view/109781070 See further recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX 2010 (6ES7671-0RC08-0YA0): All versions < V2010 SP3	Update to V2010 SP3 or later version and apply BIOS and Microsoft Windows updates https://support.industry.siemens.com/cs/ww/en/view/109765109/ See further recommendations from section Workarounds and Mitigations

SIMATIC WinAC RTX F 2010 (6ES7671-1RC08-0YA0): All versions < V2010 SP3	Update to V2010 SP3 or later version and apply BIOS and Microsoft Windows updates https://support.industry.siemens.com/cs/ww/en/view/109765109/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Advanced: All versions < V15.1 Upd4	Update to V15.1 Upd4 or later version https://support.industry.siemens.com/cs/ww/en/view/109763891/ See further recommendations from section Workarounds and Mitigations
SIMOCODE pro V Ethernet/IP (incl. SIPLUS variants): All versions < V1.1.3	Update to V1.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109756912/ See further recommendations from section Workarounds and Mitigations
SIMOCODE pro V PROFINET (incl. SIPLUS variants): All versions < V2.1.3	Update to V2.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109749989/ See further 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/ See further recommendations from section Workarounds and Mitigations
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/ See further recommendations from section Workarounds and Mitigations
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/ See further recommendations from section Workarounds and Mitigations
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 See further recommendations from section Workarounds and Mitigations
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 See further 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 or later version https://support.industry.siemens.com/cs/ww/en/view/109765015 See further recommendations from section Workarounds and Mitigations

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/ See further recommendations from section Workarounds and Mitigations
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/ See further 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/ See further recommendations from section Workarounds and Mitigations
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 See further recommendations from section Workarounds and Mitigations
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 See further 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 or later version https://support.industry.siemens.com/cs/ww/en/view/109765015 See further recommendations from section Workarounds and Mitigations
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 See further recommendations from section Workarounds and Mitigations
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 See further recommendations from section Workarounds and Mitigations
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 See further recommendations from section Workarounds and Mitigations
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 See further recommendations from section Workarounds and Mitigations

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 See further recommendations from section Workarounds and Mitigations
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 See further recommendations from section Workarounds and Mitigations
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/ See further recommendations from section Workarounds and Mitigations
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/ See further 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/ See further recommendations from section Workarounds and Mitigations
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 See further recommendations from section Workarounds and Mitigations
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 See further 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 or later version https://support.industry.siemens.com/cs/ww/en/view/109765015 See further recommendations from section Workarounds and Mitigations
SINAMICS S210: All versions < V5.1 SP1 HF8	Update to V5.1 SP1 HF8 or later version https://support.industry.siemens.com/cs/ww/en/view/109781700/ See recommendations from section Workarounds and Mitigations
SIPLUS ET 200S IM151-8 PN/DP CPU (6AG1151-8AB01-7AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/47353723/ See further recommendations from section Workarounds and Mitigations

SIPLUS ET 200S IM151-8F PN/DP CPU (6AG1151-8FB01-2AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/47354354/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 443-1 (6AG1443-1EX30-4XE0): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 314C-2 PN/DP (6AG1314-6EH04-7AB0): All versions < V3.3.16	Update to V3.3.16 or later version https://support.industry.siemens.com/cs/ww/en/view/51466769/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 315-2 PN/DP (6AG1315-2EH14-7AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/40360647/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 315F-2 PN/DP (6AG1315-2FJ14-2AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/40944925/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 317-2 PN/DP (6AG1317-2EK14-7AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/40362228/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 317F-2 PN/DP (6AG1317-2FK14-2AB0): All versions < V3.2.16	Update to V3.2.16 or later version https://support.industry.siemens.com/cs/ww/en/view/40945128/ See further recommendations from section Workarounds and Mitigations
SITOP Manager: All versions < V1.1	Update to V1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109760607/ See further recommendations from section Workarounds and Mitigations

SITOP PSU8600: All versions < V1.5	Update to V1.5 or later version https://support.industry.siemens.com/cs/ww/en/view/102295547/ See further recommendations from section Workarounds and Mitigations
SITOP UPS1600 (incl. SIPLUS variants): All versions < V2.3	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/79207181/ See further 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/ See further 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 the integrated webserver
- Deactivate the webserver if not required, and if deactivation is supported by the product

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the 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

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

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 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).

SCALANCE M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 are industrial routers.

SIMATIC CP 343-1 and CP 443-1 are communication processors (CP) designed to enable Ethernet communication for SIMATIC S7-300/S7-400 CPUs.

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

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 RF180C is an RFID communication module for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet. SIMATIC RF180C is superseded by the SIMATIC RF18xC devices (RF185C, RF186C, RF188C).

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).

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

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

SIMATIC S7-PLCSIM Advanced simulates S7-1200, S7-1500 and a few other PLC derivatives. Includes full network access to simulate the PLCs, even in virtualized environments.

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

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

SIMOCODE pro is a modular motor management system that combines all required protection, monitoring, safety and control functions for motor feeders.

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

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.

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

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.

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-2019-6568

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.

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 party for its 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 RF182C and RFID 181EIP
V2.1 (2020-12-08):	Updated information regarding successor products for SIMATIC RF182C and RFID 181EIP
V2.2 (2022-02-08):	No remediation planned for SIMATIC CP 343-1 Advanced, SIMATIC CP 443-1 OPC UA, SIMATIC CP 1604, SIMATIC CP 1616, and SIPLUS NET CP 343-1 Advanced
V2.3 (2022-06-14):	No fix planned for SIMATIC CP 443-1 Advanced and SIPLUS NET CP 443-1 Advanced
V2.4 (2022-08-09):	No fix planned for SIMATIC S7-400 PN/DP V6 and below CPU family; consolidated mitigation measures

V2.5 (2023-01-10):	SIMATIC S7-300 CPU family expanded with product specific designations, patch links and MLFBs and Name of SIMOCODE pro V EIP (incl. SIPLUS variants) was updated to SIMOCODE pro V Ethernet/IP (incl. SIPLUS variants) and Name of SIMOCODE pro V PN (incl. SIPLUS variants) was updated to SIMOCODE pro V PROFINET (incl. SIPLUS variants); No fix planned for SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)
V2.6 (2023-04-11):	Added fix for SIMATIC CP 443-1 and CP 443-1 Advanced and for SINAMICS S210
V2.7 (2023-05-09):	Updated fix information for SINAMICS S210

TERMS OF USE