SSA-592007: Denial of Service Vulnerability in Industrial Products

Publication Date: 2018-03-20
Last Update: 2023-05-09
Current Version: V2.1
CVSS v3.1 Base Score: 6.5

SUMMARY

Several industrial controllers are affected by a security vulnerability that could allow an attacker to cause a denial of service condition via PROFINET DCP network packets under certain circumstances. Precondition for this scenario is a direct OSI Layer 2 access to the affected products. PROFIBUS interfaces are not affected.

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 S7-400 CPU 414-3 PN/DP V7 (6ES7414-3EM07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 414F-3 PN/DP V7 (6ES7414-3FM07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416-3 PN/DP V7 (6ES7416-3ES07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416F-3 PN/DP V7 (6ES7416-3FS07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Advanced (incl. SIPLUS variants): 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 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 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 CPU 412-2 PN V7 (6ES7412-2EK07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants): All versions < V6.0.9	Update to V6.0.9 https://support.industry.siemens.com/cs/ww/en/view/109474550 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants): All versions < V6.0.7	Update to V6.0.7 https://support.industry.siemens.com/cs/ww/en/view/109474874 See further recommendations from section Workarounds and Mitigations

SIMATIC S7-410 CPU family (incl. SIPLUS variants): All versions < V8.1	Update to V8.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109476571 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V1.7.0	Update to V1.7.0 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 < V1.7.0	Update to V1.7.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109478528/ 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
SINUMERIK 828D: All versions < V4.7 SP6 HF1	Update to V4.7 SP6 HF1 or later version SINUMERIK software can be obtained from your local Siemens account manager See further 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 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
SIPLUS S7-400 CPU 414-3 PN/DP V7 (6AG1414-3EM07-7AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIPLUS S7-400 CPU 416-3 PN/DP V7 (6AG1416-3ES07-7AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
Softnet PROFINET IO for PC-based Windows systems: All versions	Currently no fix is planned 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:

- Use VPN for protecting network communication between cells.

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

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

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

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

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.

Softnet PROFINET IO for PC-based Windows systems allows setting up open control solutions on standard PC hardware.

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-2018-4843

Responding to a PROFINET DCP request with a specially crafted PROFINET DCP packet could cause a denial of service condition of the requesting system.

The security vulnerability could be exploited by an attacker located on the same Ethernet segment (OSI Layer 2) as the targeted device. A manual restart is required to recover the system.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

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 (2018-03-20):	Publication Date
V1.1 (2018-03-27):	Removed SINUMERIK 840D sl from affected products
V1.2 (2018-10-09):	Added update for SINUMERIK 828D
V1.3 (2019-01-08):	Added update for SIMATIC S7-300 incl. F and T
V1.4 (2019-05-14):	Added update for S7-400 H V6
V1.5 (2019-10-08):	Renamed SIMATIC WinAC RTX 2010 incl. F to SIMATIC WinAC RTX (F) 2010 and added update information for SIMATIC WinAC RTX (F) 2010
V1.6 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products
V1.7 (2022-06-14):	No fix planned for SIMATIC CP 343-1 and SIMATIC CP 443-1 Advanced
V1.8 (2022-08-09):	Clarify no fix planned for SIMATIC CP 343-1 Advanced (incl. SIPLUS variants)
V1.9 (2023-01-10):	SIMATIC S7-300 CPU family expanded with product specific designations, patch links and MLFBs; No fix planned for SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)
V2.0 (2023-04-11):	Added fix for SIMATIC CP 443-1 and CP 443-1 Advanced
V2.1 (2023-05-09):	Added fix for SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants); expanded SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) to individual products and MLFBs; reviewed CVSS score and description of CVE-2018-4843

TERMS OF USE