SSA-473245: Denial of Service Vulnerability in Profinet Devices

Publication Date: 2019-10-08
Last Update: 2023-05-09
Current Version: V2.6
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability in affected devices could allow an attacker to perform a denial of service attack if a large amount of specially crafted UDP packets are sent to the device.

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
Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All versions < V4.6 Patch 01	Update to V4.6 Patch 01 or later version https://support.industry.siemens.com/cs/ww/en/view/109781345/ See further recommendations from section Workarounds and Mitigations

SIMATIC CFU PA (6ES7655-5PX11-0XX0): All versions < V1.2.0	Update to V1.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109754628/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200AL: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 4AO U/I 4xM12 (6ES7145-6HD00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8 DIO, DC24V/1,3A, 8xM12 (6ES7147-6BG00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8 DO, DC24V/2A, 8xM12 (6ES7142-6BR00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8AI RTD/TC 8xM12 (6ES7144-6KD50-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8AI; 4 U/I; 4 RTD/TC 8xM12 (6ES7144-6KD00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DI, DC24V, 4xM12 (6ES7141-6BF00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DI, DC24V, 8xM12 (6ES7141-6BG00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/0,5A, 4xM12 (6ES7142-6BF50-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 4xM12 (6ES7142-6BF00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 8xM12 (6ES7142-6BG00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 16DI, DC24V, 8xM12 (6ES7141-6BH00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC ET200ecoPN, 16DO DC24V/1,3A, 8xM12 (6ES7142-6BH00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN: IO-Link Master (6ES7148-6JA00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200M (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200MP IM155-5 PN BA (incl. SIPLUS variants): All versions < V4.3.0	Update to V4.3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109754281/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants): All versions < V4.4.0	Update to V4.4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200MP IM155-5 PN ST (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200pro: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200S (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN BA (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HA (incl. SIPLUS variants): All versions < V1.2.1	Update to V1.2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109763483/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants): All versions < V4.2.2	Update to V4.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HS (incl. SIPLUS variants): All versions < V4.0.1	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109795369/ See further recommendations from section Workarounds and Mitigations

SIMATIC ET200SP IM155-6 PN ST (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN/2 HF (incl. SIPLUS variants): All versions < V4.2.2	Update to V4.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109769765/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN/3 HF (incl. SIPLUS variants): All versions < V4.2.1	Update to V4.2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109769419/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM154-8 PN/DP CPU (6ES7154-8AB01-0AB0): All versions < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 PC (incl. SIPLUS variants): All versions < V2.0	Update to V2.0 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC HMI KTP Mobile Panels: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PN/PN Coupler (6ES7158-3AD10-0XA0): All versions < V4.2.1	Update to V4.2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109760973/ See further recommendations from section Workarounds and Mitigations
SIMATIC PROFINET Driver: All versions < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109768047/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 314C-2 PN/DP (6ES7314-6EH04-0AB0): All versions < V3.3.17	Update to V3.3.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 or later version https://support.industry.siemens.com/cs/ww/en/view/109474550/ 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 S7-410 V8 CPU family (incl. SIPLUS variants): All versions < V8.2.2	Update to V8.2.2 or later version https://support.industry.siemens.com/cs/us/en/view/109476571/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.4.0	Update to V4.4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109763919/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.0	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109764666/ See further recommendations from section Workarounds and Mitigations

SIMATIC TDC CP51M1: All versions < V1.1.8	Update to V1.1.8 or later version https://support.industry.siemens.com/cs/ww/en/view/27049282/ See recommendations from section Workarounds and Mitigations
SIMATIC TDC CPU555: All versions < V1.1.1	Update to V1.1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109740119/ See 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
SINAMICS DCM: All versions < V1.5 HF1	Update to V1.5 HF1 or later version https://support.industry.siemens.com/cs/ww/en/view/44029688/ See further recommendations from section Workarounds and Mitigations
SINAMICS DCP: All versions < V1.3	Update to V1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109773826/ See further recommendations from section Workarounds and Mitigations
SINAMICS G110M V4.7 PN Control Unit: All versions < V4.7 SP10 HF5	Update to V4.7 SP10 HF5 or later version https://support.industry.siemens.com/cs/ww/en/view/109756820/ See further recommendations from section Workarounds and Mitigations
SINAMICS G120 V4.7 PN Control Unit (incl. SIPLUS variants): All versions < V4.7 SP10 HF5	Update to V4.7 SP10 HF5 or later version https://support.industry.siemens.com/cs/ww/en/view/109756820/ See further recommendations from section Workarounds and Mitigations
SINAMICS G130 V4.7 Control Unit: All versions < 4.8	Upgrade to V5.2 HF1 https://support.industry.siemens.com/cs/ww/en/view/109764679/ See further recommendations from section Workarounds and Mitigations
SINAMICS G150 Control Unit: All versions < 4.8	Upgrade to V5.2 HF1 https://support.industry.siemens.com/cs/ww/en/view/109764679/ See further recommendations from section Workarounds and Mitigations

SINAMICS GH150 V4.7 Control Unit: All versions	Upgrade to V4.8 SP2 HF9 The update can be obtained from your Siemens representative or via Siemens customer service. See further recommendations from section Workarounds and Mitigations
SINAMICS GL150 V4.7 Control Unit: All versions	Upgrade to V4.8 SP2 HF9 The update can be obtained from your Siemens representative or via Siemens customer service. See further recommendations from section Workarounds and Mitigations
SINAMICS GM150 V4.7 Control Unit: All versions	Upgrade to V4.8 SP2 HF9 The update can be obtained from your Siemens representative or via Siemens customer service. See further recommendations from section Workarounds and Mitigations
SINAMICS S110 Control Unit: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SINAMICS S120 V4.7 Control Unit (incl. SIPLUS variants): All versions	Upgrade to V5.2 HF4 https://support.industry.siemens.com/cs/ww/en/view/109762626/ See further recommendations from section Workarounds and Mitigations
SINAMICS S150 Control Unit: All versions < 4.8	Upgrade to V5.2 HF1 https://support.industry.siemens.com/cs/ww/en/view/109764679/ See further recommendations from section Workarounds and Mitigations
SINAMICS SL150 V4.7 Control Unit: All versions < V4.7 HF33	Update to V4.7 HF33 or later version The update can be obtained from your Siemens representative or via Siemens customer service. See further recommendations from section Workarounds and Mitigations
SINAMICS SM120 V4.7 Control Unit: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SINUMERIK 828D: All versions < V4.8 SP5	Update to V4.8 SP5 or later version The update can be obtained from your Siemens representative or via Siemens customer service. See further recommendations from section Workarounds and Mitigations
SINUMERIK 840D sl: All versions < V4.8 SP6	Update to V4.8 SP6 or later version The update can be obtained from your Siemens representative or via Siemens customer service. See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200S IM151-8 PN/DP CPU (6AG1151-8AB01-7AB0): All versions < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 or later version https://support.industry.siemens.com/cs/ww/en/view/47354354/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET PN/PN Coupler (6AG2158-3AD10-4XA0): All versions < V4.2.1	Update to V4.2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109760973/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 314C-2 PN/DP (6AG1314-6EH04-7AB0): All versions < V3.3.17	Update to V3.3.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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 < V3.2.17	Update to V3.2.17 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

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

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

Development/Evaluation Kits for PROFINET IO are used to develop compact or modular PROFINET field devices.

PN/PN coupler is used for connecting two PROFINET networks.

SIMATIC Compact Field Unit (SIMATIC CFU) is a smart field distributor for use as an I/O device on PROFINET of an automation system.

SIMATIC ET 200 Interface modules for PROFINET IO are used to connect field devices (IO Devices) to controllers (IO Controller) via PROFINET.

PROFINET Driver is a development kit used to develop PROFINET IO controllers.

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 TDC is a multiprocessor automation system for drive, control and technology tasks. The system is used particularly for large plants.

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

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

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.

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-2019-10936

Affected devices improperly handle large amounts of specially crafted UDP packets.

This could allow an unauthenticated remote attacker to trigger a denial of service condition.

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-400: Uncontrolled Resource Consumption

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 (2019-10-08):	Publication Date
V1.1 (2019-11-12):	Added solution for SINAMICS S120 V4.7, SINAMICS S150, SINAMICS G130 V4.7, SINAMICS G150 and SINAMICS SL150 V4.7
V1.2 (2020-01-14):	Added solution for SIMATIC S7-1200 and S7-1500 Software and Open Controller. SIPLUS devices now explicitly mentioned in the list of affected products
V1.3 (2020-02-11):	Added solution for SINAMICS DCP
V1.4 (2020-03-10):	Added solution for SIMATIC S7-300 CPU family
V1.5 (2020-04-14):	Added solution for SIMATIC ET200MP IM155-5 PN HF
V1.6 (2020-07-14):	Added SIMATIC TDC CP51M1 and CPU555 to the list of affected products
V1.7 (2020-08-11):	Added solution for SIMATIC PN/PN Coupler. Added SIMATIC ET200ecoPN product variants (MLFB IDs) that are not affected
V1.8 (2020-09-08):	Added solution for EK-ERTEC 200P and S7-410 V8
V1.9 (2021-01-12):	Added solution for SIMATIC ET200SP IM155-6 PN HA and added ecoPN model (6ES7148-6JG00-0BB0) as not affected
V2.0 (2021-06-08):	Added solution for SIMATIC ET200SP IM155-6 PN HS
V2.1 (2021-10-12):	Clarified affected ET200ecoPN models
V2.2 (2022-02-08):	Clarified that no remediation is planned for ET200 devices
V2.3 (2022-08-09):	No fix planned for SIMATIC S7-400 PN/DP V6 and below CPU family
V2.4 (2022-12-13):	Added fix for SINUMERK 840D sl; no fix planned for PROFINET development/evaluation kits - DK Standard Ethernet Controller and EK-ERTEC 200; SIMATIC S7-300 CPU family expanded with product specific designations, patch links and MLFBs
V2.5 (2023-01-10):	No fix planned for remaining products
V2.6 (2023-05-09):	Expanded SIMATIC S7-400 V7 CPU family (incl. SIPLUS variants) to individual products and MLFBs; added fix for SIMATIC S7-400 PN/DP V7 CPUs; clarified that other S7-400 V7 CPUs are not affected

TERMS OF USE

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.