SSA-346262: Denial-of-Service in Industrial Products

Publication Date: 2017-11-23
Last Update: 2020-08-11
Current Version: V2.8
CVSS v3.1 Base Score: 7.5

SUMMARY

Several industrial products are affected by a vulnerability that could allow remote attackers to conduct a Denial-of-Service (DoS) attack by sending specially crafted packets to port 161/udp (SNMP).

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
SIMATIC S7-200 Smart: All versions < V2.03.01	Update to V2.03.01 https://support.industry.siemens.com/cs/cn/en/view/109749409
SIMATIC S7-400 PN/DP V6 CPU family and below (incl. SIPLUS variants): All versions < V6.0.6	Update to V6.0.6 https://support.industry.siemens.com/cs/de/en/view/109474874
SIMATIC S7-400 H V6 CPU family and below (incl. SIPLUS variants): All versions < V6.0.8	Update to V6.0.8 https://support.industry.siemens.com/cs/ww/en/view/109474550
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions < V7.0.2	Update to V7.0.2 https://support.industry.siemens.com/cs/ww/en/view/109752685
SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants): All versions < V8.2.1	Update to V8.2.1 https://support.industry.siemens.com/cs/ww/en/view/109476571
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 S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.2.3	Update to V4.2.3 https://support.industry.siemens.com/cs/us/en/view/109741461
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.0	Upgrade to V2.0 or newer https://support.industry.siemens.com/cs/us/en/ps/13717/dl
SIMATIC S7-1500 Software Controller: All versions < V2.0	Upgrade to V2.0 or newer https://support.industry.siemens.com/cs/us/en/view/109478528

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 ET200AL: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN (except 6ES7141-6BG00-0BB0, 6ES7141-6BH00-0BB0, 6ES7142-6BG00-0BB0, 6ES7142-6BR00-0BB0, 6ES7143-6BH00-0BB0, 6ES7146-6FF00-0AB0 and 6ES7148-6JD00-0AB0): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200M (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200MP IM155-5 PN BA (incl. SIPLUS variants): All versions < V4.0.2	Update to V4.0.2 https://support.industry.siemens.com/cs/ww/en/view/109754281
SIMATIC ET200MP IM155-5 PN ST (incl. SIPLUS variants): All versions < V4.1	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/78647504
SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants): All versions < V4.2	Update to V4.2 https://support.industry.siemens.com/cs/us/en/view/93012181
SIMATIC ET200pro: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200S (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants): All versions < V4.2.0	Update to V4.2.0 https://support.industry.siemens.com/cs/ww/en/view/85624387
SIMATIC ET200SP IM155-6 PN HA (incl. SIPLUS variants): All versions < V1.1.0	Update to V1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109763483
SIMATIC ET200SP IM155-6 PN BA (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN ST (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HS (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations

SIMATIC TDC CPU555: All versions < V1.1.1	Update to V1.1.1 https://support.industry.siemens.com/cs/ww/en/view/109740119
SIMATIC TDC CP51M1: All versions < V1.1.8	Update to V1.1.8 https://support.industry.siemens.com/cs/ww/en/view/27049282
Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller: All versions < V4.1.1 Patch 05	Update to V4.1.1 Patch 05 https://support.industry.siemens.com/cs/ww/en/view/109755160
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All versions < V4.5	Update to V4.5 https://support.industry.siemens.com/cs/ww/en/view/109750012
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All versions < V4.5	Update to V4.5 https://support.industry.siemens.com/cs/ww/en/view/109755151
SIMOTION D (incl. SIPLUS variants): All versions < V5.1 HF1	Update to V5.1 HF1 https://support.industry.siemens.com/cs/ww/en/view/31045047
SIMOTION C: All versions < V5.1 HF1	Update to V5.1 HF1 https://support.industry.siemens.com/cs/ww/en/view/31263919
SIMOTION P V4.4 and V4.5: All versions < V4.5 HF5	Update to V4.5 HF5 Please contact your Siemens representative for information on how to obtain the update.
SIMOTION P V5: All versions < V5.1 HF1	Update to V5.1 HF1 Please contact your Siemens representative for information on how to obtain the update.
SINAMICS DCM w. PN: All versions < V1.4 SP1 HF6	Update to V1.4 SP1 HF6 https://support.industry.siemens.com/cs/ww/en/view/44029688
SINAMICS DCP w. PN: All versions < V1.2 HF2	Update to V1.2 HF2 https://support.industry.siemens.com/cs/ww/en/view/109474935
SINAMICS G110M w. PN: All versions < V4.7 SP9 HF1	Update to V4.7 SP9 HF1 https://support.industry.siemens.com/cs/document/109750507
SINAMICS G120(C/P/D) w. PN (incl. SIPLUS variants): All versions < V4.7 SP9 HF1	Update to V4.7 SP9 HF1 https://support.industry.siemens.com/cs/document/109750507
SINAMICS G130 V4.7 w. PN: All versions < V4.7 HF29	Update to V4.7 HF29 https://support.industry.siemens.com/cs/ww/en/view/103433117
SINAMICS G130 V4.8 w. PN: All versions < V4.8 HF4	Update to V4.8 HF4 https://support.industry.siemens.com/cs/ww/en/view/109742040

SINAMICS G150 V4.7 w. PN: All versions < V4.7 HF29	Update to V4.7 HF29 https://support.industry.siemens.com/cs/ww/en/view/103433117
SINAMICS G150 V4.8 w. PN: All versions < V4.8 HF4	Update to V4.8 HF4 https://support.industry.siemens.com/cs/ww/en/view/109742040
SINAMICS S110 w. PN: All versions < V4.4 SP3 HF6	Update to V4.4 SP3 HF6 https://support.industry.siemens.com/cs/document/109474320
SINAMICS S120 prior to V4.7 w. PN (incl. SIPLUS variants): All versions < V4.7	Update to latest version of V5.1 SP1 https://support.industry.siemens.com/cs/document/109758423
SINAMICS S120 V4.7 w. PN (incl. SIPLUS variants): All versions < V4.7 HF29	Update to V4.7 HF29 https://support.industry.siemens.com/cs/ww/en/view/92522512
SINAMICS S120 V4.7 SP1 w. PN (incl. SIPLUS variants): All versions	Update to latest version of V5.1 SP1 https://support.industry.siemens.com/cs/document/109758423
SINAMICS S120 V4.8 w. PN (incl. SIPLUS variants): All versions < V4.8 HF5	Update to V4.8 HF5 https://support.industry.siemens.com/cs/us/en/view/109740193
SINAMICS S150 V4.7 w. PN: All versions < V4.7 HF29	Update to V4.7 HF29 https://support.industry.siemens.com/cs/ww/en/view/103433117
SINAMICS S150 V4.8 w. PN: All versions < V4.8 HF4	Update to V4.8 HF4 https://support.industry.siemens.com/cs/ww/en/view/109742040
SINAMICS V90 w. PN: All versions < V1.02	Update to V1.02 https://support.industry.siemens.com/cs/document/109746210
SINUMERIK 840D sl: All versions < V4.8 SP3	Update to V4.8 SP3 The update can be obtained from your local service organization.
SIMATIC Compact Field Unit: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PN/PN Coupler (incl. SIPLUS NET variants): All versions < V4.2.0	Update to V4.2.0 https://support.industry.siemens.com/cs/ww/en/view/109760973
SIMOCODE pro V PN (incl. SIPLUS variants): All versions < V2.1.1	Update to V2.1.1 https://support.industry.siemens.com/cs/ww/en/view/109749989
SIRIUS Soft Starter 3RW44 PN: 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:

- Disable SNMP if this is supported by the product (refer to the product documentation). Disabling SNMP fully mitigates the vulnerability.
- Protect network access to port 161/udp of affected devices.
- Apply cell protection concept and implement Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security.
- Use VPN for protecting network communication between cells.

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.

The SIMATIC Compact Field Unit is a field unit for use as an IO device on the PROFINET IO network 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.

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

The S7-200 SMART series is a line of micro-programmable logic controllers that can control a variety of small automation applications.

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

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

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

SIMOTION is a scalable high performance hardware and software system for motion control.

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.

SIRIUS 3RW soft starters permit soft starting and soft rampdown of three-phase asynchronous motors.

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-2017-12741

Specially crafted packets sent to port 161/udp could cause a Denial-of-Service condition. The affected devices must be restarted manually.

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 parties for their efforts:

- George Lashenko from CyberX for coordinated disclosure of the vulnerability
- 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 (2017-11-23):	Publication Date
V1.1 (2017-12-18):	Changed affected products: V2.0 and newer of SIMATIC S7-1500 and V2.0 and newer of SIMATIC S7-1500 Software Controller are not affected. Added update information for SIMATIC S7-400 H V6
V1.2 (2018-01-18):	New advisory format, added update information for SINAMICS V90 w. PN, SINAMICS S120 and SINAMICS S110 w. PN
V1.3 (2018-01-24):	Added update for S7-400 V7 and SIMATIC ET 200MP IM155-5 PN BA
V1.4 (2018-02-22):	Added update for SIMATIC ET 200MP IM155-5 PN ST, SIMOTION P V4.4 and V4.5, and Development/Evaluation Kits for PROFINET IO DK Standard Ethernet Controller and EK-ERTEC 200, Corrected patch link for SIMOTION D
V1.5 (2018-05-03):	Added update information for V4.8 of SINAMICS G130, G150, S120 and S150
V1.6 (2018-05-15):	Added update information for V4.7 of SINAMICS G130, G150, S120 and S150
V1.7 (2018-09-11):	Added update for SINAMICS DCP w. PN and SINAMICS DCM w. PN
V1.8 (2018-10-09):	Added update for SIMATIC S7-1200 CPU

V1.9 (2018-11-13):	Updated solution for SINAMICS S120, added solution for PN/PN Coupler, SIMATIC ET200 SP, SIMATIC S7-400 V8, SIMOCODE pro V PROFINET
V2.0 (2018-12-11):	Updated solution for SIMATIC ET 200MP IM155-5 PN HF
V2.1 (2019-01-08):	Updated solution for SIMATIC S7-300
V2.2 (2019-02-12):	Updated solution for SIMATIC ET 200SP IM155-6 PN HA
V2.3 (2019-03-12):	Update for SINUMERIK 840D sl
V2.4 (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
V2.5 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products
V2.6 (2020-04-14):	Mention that SIMATIC S7-400 CPU family below V6 is vulnerable
V2.7 (2020-07-14):	Added SIMATIC TDC CP51M1 and CPU555 to the list of affected products
V2.8 (2020-08-11):	Added SIMATIC ET200ecoPN product variants (MLFB IDs) that are not affected

TERMS OF USE