SSA-346262: Denial of Service Vulnerability in SNMP Interface of Industrial Products

Publication Date: 2017-11-23
Last Update: 2024-07-09
Current Version: V3.3
CVSS v3.1 Base Score: 7.5
CVSS v4.0 Base Score: 8.7

SUMMARY

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

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller: All versions < V4.1.1 Patch 05 affected by CVE-2017-12741	Update to V4.1.1 Patch 05 https://support.industry.siemens.com/cs/ww/en/view/109755160 See further recommendations from section Workarounds and Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All versions < V4.5 affected by CVE-2017-12741	Update to V4.5 https://support.industry.siemens.com/cs/ww/en/view/109755151 See further recommendations from section Workarounds and Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All versions < V4.5 affected by CVE-2017-12741	Update to V4.5 https://support.industry.siemens.com/cs/ww/en/view/109750012 See further recommendations from section Workarounds and Mitigations
SIMATIC Compact Field Unit: All versions affected by CVE-2017-12741	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 4AO U/I 4xM12 (6ES7145-6HD00-0AB0): All versions affected by CVE-2017-12741	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 affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC ET200ecoPN, 8 DO, DC24V/2A, 8xM12 (6ES7142-6BR00-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8AI RTD/TC 8xM12 (6ES7144-6KD50-0AB0): All versions affected by CVE-2017-12741	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 affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DI, DC24V, 4xM12 (6ES7141-6BF00-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DI, DC24V, 8xM12 (6ES7141-6BG00-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/0,5A, 4xM12 (6ES7142-6BF50-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 4xM12 (6ES7142-6BF00-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 8xM12 (6ES7142-6BG00-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 16DI, DC24V, 8xM12 (6ES7141-6BH00-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 16DO DC24V/1,3A, 8xM12 (6ES7142-6BH00-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN: IO-Link Master (6ES7148-6JA00-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200S (incl. SIPLUS variants): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC ET 200AL IM 157-1 PN (6ES7157-1AB00-0AB0): All versions < V1.0.2 affected by CVE-2017-12741	Update to V1.0.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109479281/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200M (incl. SIPLUS variants): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN BA (6ES7155-5AA00-0AA0): All versions < V4.0.2 affected by CVE-2017-12741	Update to V4.0.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109754281/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN HF (incl. SIPLUS variants):	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN HF (6ES7155-5AA00-0AC0): All versions < V4.2.0 affected by CVE-2017-12741	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-2AC0): All versions < V4.2.0 affected by CVE-2017-12741	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-7AC0): All versions < V4.2.0 affected by CVE-2017-12741	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN HF T1 RAIL (6AG2155-5AA00-1AC0): All versions < V4.2.0 affected by CVE-2017-12741	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/93012181/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN ST (incl. SIPLUS variants):	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations

SIMATIC ET 200MP IM 155-5 PN ST (-Ax00) (incl. SIPLUS variants):	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200MP IM 155-5 PN ST (6ES7155-5AA00-0AB0): All versions < V4.1.0 affected by CVE-2017-12741	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN ST (6AG1155-5AA00-7AB0): All versions < V4.1.0 affected by CVE-2017-12741	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200MP IM 155-5 PN ST TX RAIL (6AG2155-5AA00-4AB0): All versions < V4.1.0 affected by CVE-2017-12741	Update to V4.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM 154-3 PN HF (6ES7154-3AB00-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM 154-4 PN HF (6ES7154-4AB10-0AB0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN BA (6ES7155-6AR00-0AN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN HA (incl. SIPLUS variants): All versions < V1.1.0 affected by CVE-2017-12741	Update to V1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109763483 See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN HF (incl. SIPLUS variants):	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations

SIMATIC ET 200SP IM 155-6 PN HF (6ES7155-6AU00-0CN0): All versions < V4.2.0 affected by CVE-2017-12741	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU00-4CN0): All versions < V4.2.0 affected by CVE-2017-12741	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU00-2CN0): All versions < V4.2.0 affected by CVE-2017-12741	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN HF T1 RAIL (6AG2155-6AU00-1CN0): All versions < V4.2.0 affected by CVE-2017-12741	Update to V4.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/85624387/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN HS (6ES7155-6AU00-0DN0): All versions < V4.0.1 affected by CVE-2017-12741	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 ET 200SP IM 155-6 PN ST (incl. SIPLUS variants):	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST (-Ax00) (incl. SIPLUS variants):	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST (6ES7155-6AU00-0BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST BA (6ES7155-6AA00-0BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST (6AG1155-6AU00-7BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPLUS ET 200SP IM 155-6 PN ST BA (6AG1155-6AA00-7BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST BA TX RAIL (6AG2155-6AA00-4BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST TX RAIL (6AG2155-6AU00-4BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST (-Ax01) (incl. SIPLUS variants):	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST (6ES7155-6AU01-0BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP IM 155-6 PN ST BA (6ES7155-6AA01-0BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST (6AG1155-6AU01-7BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST BA (6AG1155-6AA01-7BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST BA TX RAIL (6AG2155-6AA01-4BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP IM 155-6 PN ST TX RAIL (6AG2155-6AU01-4BN0): All versions affected by CVE-2017-12741	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PN/PN Coupler (incl. SIPLUS NET variants): All versions < V4.2.0 affected by CVE-2017-12741	Update to V4.2.0 https://support.industry.siemens.com/cs/ww/en/view/109760973 See further recommendations from section Workarounds and Mitigations

SIMATIC S7-200 SMART: All versions < V2.03.01 affected by CVE-2017-12741	Update to V2.03.01 https://support.industry.siemens.com/cs/cn/en/view/109749409 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V3.X.16 affected by CVE-2017-12741	Update to V3.X.16 or later version https://support.industry.siemens.com/cs/ww/en/ps/13752/dl See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H V6 and below CPU family (incl. SIPLUS variants): All versions < V6.0.8 affected by CVE-2017-12741	Update to V6.0.8 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 < V6.0.6 affected by CVE-2017-12741	Update to V6.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109474874/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions < V7.0.2 affected by CVE-2017-12741	Update to V7.0.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants): All versions < V8.2.1 affected by CVE-2017-12741	Update to V8.2.1 https://support.industry.siemens.com/cs/ww/en/view/109476571 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.2.3 affected by CVE-2017-12741	Update to V4.2.3 https://support.industry.siemens.com/cs/us/en/view/109741461 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.0 affected by CVE-2017-12741	Upgrade to V2.0 or newer https://support.industry.siemens.com/cs/us/en/ps/13717/dl See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 Software Controller: All versions < V2.0 affected by CVE-2017-12741	Upgrade to V2.0 or newer https://support.industry.siemens.com/cs/us/en/view/109478528 See further recommendations from section Workarounds and Mitigations
SIMATIC TDC CP51M1: All versions < V1.1.8 affected by CVE-2017-12741	Update to V1.1.8 or later version https://support.industry.siemens.com/cs/ww/en/view/27049282/ See further recommendations from section Workarounds and Mitigations
SIMATIC TDC CPU555: All versions < V1.1.1 affected by CVE-2017-12741	Update to V1.1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109740119/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX 2010 (6ES7671-0RC08-0YA0): All versions < V2010 SP3 affected by CVE-2017-12741	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 affected by CVE-2017-12741	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
SIMOCODE pro V PROFINET (incl. SIPLUS variants): All versions < V2.1.1 affected by CVE-2017-12741	Update to V2.1.1 https://support.industry.siemens.com/cs/ww/en/view/109749989 See further recommendations from section Workarounds and Mitigations
SIMOTION C: All versions < V5.1 HF1 affected by CVE-2017-12741	Update to V5.1 HF1 https://support.industry.siemens.com/cs/ww/en/view/31263919 See further recommendations from section Workarounds and Mitigations
SIMOTION D: All versions < V5.1 HF1 affected by CVE-2017-12741	Update to V5.1 HF1 https://support.industry.siemens.com/cs/ww/en/view/31045047 See further recommendations from section Workarounds and Mitigations

SIMOTION P V4.4 and V4.5: All versions < V4.5 HF5 affected by CVE-2017-12741	Update to V4.5 HF5 Please contact your Siemens representative for information on how to obtain the update. See further recommendations from section Workarounds and Mitigations
SIMOTION P V5: All versions < V5.1 HF1 affected by CVE-2017-12741	Update to V5.1 HF1 Please contact your Siemens representative for information on how to obtain the update. See further recommendations from section Workarounds and Mitigations
SINAMICS DCM w. PN: All versions < V1.4 SP1 HF6 affected by CVE-2017-12741	Update to V1.4 SP1 HF6 https://support.industry.siemens.com/cs/ww/en/view/44029688 See further recommendations from section Workarounds and Mitigations
SINAMICS DCP w. PN: All versions < V1.2 HF2 affected by CVE-2017-12741	Update to V1.2 HF2 https://support.industry.siemens.com/cs/ww/en/view/109474935 See further recommendations from section Workarounds and Mitigations
SINAMICS G110M w. PN: All versions < V4.7 SP9 HF1 affected by CVE-2017-12741	Update to V4.7 SP9 HF1 https://support.industry.siemens.com/cs/document/109750507 See further recommendations from section Workarounds and Mitigations
SINAMICS G120(C/P/D) w. PN (incl. SIPLUS variants): All versions < V4.7 SP9 HF1 affected by CVE-2017-12741	Update to V4.7 SP9 HF1 https://support.industry.siemens.com/cs/document/109750507 See further recommendations from section Workarounds and Mitigations
SINAMICS G130 V4.7 w. PN: All versions < V4.7 HF29 affected by CVE-2017-12741	Update to V4.7 HF29 https://support.industry.siemens.com/cs/ww/en/view/103433117 See further recommendations from section Workarounds and Mitigations
SINAMICS G130 V4.8 w. PN: All versions < V4.8 HF4 affected by CVE-2017-12741	Update to V4.8 HF4 https://support.industry.siemens.com/cs/ww/en/view/109742040 See further recommendations from section Workarounds and Mitigations

SINAMICS G150 V4.7 w. PN: All versions < V4.7 HF29 affected by CVE-2017-12741	Update to V4.7 HF29 https://support.industry.siemens.com/cs/ww/en/view/103433117 See further recommendations from section Workarounds and Mitigations
SINAMICS G150 V4.8 w. PN: All versions < V4.8 HF4 affected by CVE-2017-12741	Update to V4.8 HF4 https://support.industry.siemens.com/cs/ww/en/view/109742040 See further recommendations from section Workarounds and Mitigations
SINAMICS S110 w. PN: All versions < V4.4 SP3 HF6 affected by CVE-2017-12741	Update to V4.4 SP3 HF6 https://support.industry.siemens.com/cs/document/109474320 See further recommendations from section Workarounds and Mitigations
SINAMICS S120 prior to V4.7 w. PN (incl. SIPLUS variants): All versions < V4.7 affected by CVE-2017-12741	Update to latest version of V5.1 SP1 https://support.industry.siemens.com/cs/document/109758423 See further recommendations from section Workarounds and Mitigations
SINAMICS S120 V4.7 SP1 w. PN (incl. SIPLUS variants): All versions affected by CVE-2017-12741	Update to latest version of V5.1 SP1 https://support.industry.siemens.com/cs/document/109758423 See further recommendations from section Workarounds and Mitigations
SINAMICS S120 V4.7 w. PN (incl. SIPLUS variants): All versions < V4.7 HF29 affected by CVE-2017-12741	Update to V4.7 HF29 https://support.industry.siemens.com/cs/ww/en/view/92522512 See further recommendations from section Workarounds and Mitigations
SINAMICS S120 V4.8 w. PN (incl. SIPLUS variants): All versions < V4.8 HF5 affected by CVE-2017-12741	Update to V4.8 HF5 https://support.industry.siemens.com/cs/us/en/view/109740193 See further recommendations from section Workarounds and Mitigations
SINAMICS S150 V4.7 w. PN: All versions < V4.7 HF29 affected by CVE-2017-12741	Update to V4.7 HF29 https://support.industry.siemens.com/cs/ww/en/view/103433117 See further recommendations from section Workarounds and Mitigations

SINAMICS S150 V4.8 w. PN: All versions < V4.8 HF4 affected by CVE-2017-12741	Update to V4.8 HF4 https://support.industry.siemens.com/cs/ww/en/view/109742040 See further recommendations from section Workarounds and Mitigations
SINAMICS V90 w. PN: All versions < V1.02 affected by CVE-2017-12741	Update to V1.02 https://support.industry.siemens.com/cs/document/109746210 See further recommendations from section Workarounds and Mitigations
SINUMERIK 840D sl: All versions < V4.8 SP3 affected by CVE-2017-12741	Update to V4.8 SP3 The update can be obtained from your local service organization. See further recommendations from section Workarounds and Mitigations
SIRIUS Soft Starter 3RW44 PN: All versions affected by CVE-2017-12741	Currently no fix is available 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.

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.

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.

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

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

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.

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

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

With the SINAMICS converter series you can solve drive tasks in the low, medium and DC voltage range.

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.

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

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-400: Uncontrolled Resource Consumption

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned
- George Lashenko from CyberX for coordinated disclosure of the vulnerability

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
V2.9 (2021-03-09):	Added ecoPN model (6ES7148-6JG00-0BB0) as not affected
V3.0 (2021-06-08):	Updated solution for SIMATIC ET200SP IM155-6 PN HS
V3.1 (2021-10-12):	Clarified affected ET200ecoPN models
V3.2 (2022-02-08):	Clarified that no remediation is planned for ET200 devices
V3.3 (2024-07-09):	Listed affected products individually instead of product families (e.g., for SIMATIC ET 200AL/MP/SP/pro IM families); added affected SIPLUS devices (e.g., SIPLUS ET 200xx IM)

TERMS OF USE