SSA-293562: Denial of Service Vulnerabilities in PROFINET DCP Implementation of Industrial Products

Publication Date:	2017-05-08
Last Update:	2022-02-08
Current Version:	V3.4
CVSS v3.1 Base Score:	6.5

SUMMARY

Several industrial devices are affected by two vulnerabilities that could allow an attacker to cause a denial of service condition via PROFINET DCP network packets under certain circumstances. The precondition for this scenario is a direct 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 new versions. Siemens recommends specific countermeasures for products where updates 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 Patch04	Update to V4.1.1 Patch04 or newer 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 < V4.2.1 Patch03	Update to V4.2.1 Patch03 or newer 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 < V4.4.0 Patch01	Update to V4.4.0 Patch01 or newer https://support.industry.siemens.com/cs/ww/en/view/109750012/ See further recommendations from section Workarounds and Mitigations
IE/AS-i Link PN IO: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
IE/PB-Link (incl. SIPLUS NET variants): All versions < V3.0	Upgrade to V3.0 https://support.industry.siemens.com/cs/ww/en/view/109744504/ See further recommendations from section Workarounds and Mitigations
SCALANCE M-800 / S615: All versions < V4.03	Update to V5.00 https://support.industry.siemens.com/cs/ww/en/view/109757544/ See further recommendations from section Workarounds and Mitigations

SCALANCE W700: All versions < V6.1	Update to V6.3.1 https://support.industry.siemens.com/cs/ww/en/view/109760470/ See further recommendations from section Workarounds and Mitigations
SCALANCE X408: All versions < V4.1.0	Update to V4.1.2 https://support.industry.siemens.com/cs/ww/en/view/109753720/ See further recommendations from section Workarounds and Mitigations
SCALANCE X414: All versions < V3.10.2	Update to V3.10.2 https://support.industry.siemens.com/cs/ww/en/view/109747276/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-200 switch family (incl. SIPLUS NET variants): All versions < V5.2.2	Update to V5.2.2 https://support.industry.siemens.com/cs/ww/en/view/109752018/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All versions < V5.4.0	Update to V5.4.0 https://support.industry.siemens.com/cs/ww/en/view/109755950/ See further recommendations from section Workarounds and Mitigations
SCALANCE X-300 switch family (incl. SIPLUS NET variants): All versions < V4.1.0	Update to V4.1.2 https://support.industry.siemens.com/cs/ww/en/view/109753720/ See further recommendations from section Workarounds and Mitigations
SCALANCE XM-400 Family: All versions < V6.1	Update to V6.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109761424/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR-500 Family: All versions < V6.1	Update to V6.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109761425/ See further recommendations from section Workarounds and Mitigations
SIMATIC CM 1542-1: All versions < V2.0	Update to V2.0 https://support.industry.siemens.com/cs/ww/en/view/109744924/ See further recommendations from section Workarounds and Mitigations
SIMATIC CM 1542SP-1: All versions < V1.0.15	Update to V1.0.15 https://support.industry.siemens.com/cs/ww/en/view/109749255/ See further recommendations from section Workarounds and Mitigations

SIMATIC CP 343-1 (incl. SIPLUS variants): All versions < V3.1.3	Update to V3.1.3 https://support.industry.siemens.com/cs/ww/en/view/109756088/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Advanced (incl. SIPLUS variants): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Lean (incl. SIPLUS variants): All versions < V3.1.3	Update to V3.1.3 https://support.industry.siemens.com/cs/ww/en/view/109756088/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 (incl. SIPLUS variants): All versions < V3.2.17	Update to V3.2.17 https://support.industry.siemens.com/cs/ww/en/view/109745387/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced (incl. SIPLUS variants): All versions < V3.2.17	Update to V3.2.17 https://support.industry.siemens.com/cs/ww/en/view/109745388/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 OPC UA: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 (incl. SIPLUS variants): All versions < V2.1.82	Update to V3.1 https://support.industry.siemens.com/cs/ww/en/view/109757489/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 IEC (incl. SIPLUS variants): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 IRC (incl. SIPLUS variants): All versions < V2.1.82	Update to V3.1 https://support.industry.siemens.com/cs/ww/en/view/109757489/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1542SP-1 IRC (incl. SIPLUS variants): All versions < V1.0.15	Update to V1.0.15 https://support.industry.siemens.com/cs/ww/en/view/109749255/ See further recommendations from section Workarounds and Mitigations

SIMATIC CP 1543-1 (incl. SIPLUS variants): All versions < V2.1	Update to V2.1 https://support.industry.siemens.com/cs/ww/en/view/109747253/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1543SP-1 (incl. SIPLUS variants): All versions < V1.0.15	Update to V1.0.15 https://support.industry.siemens.com/cs/ww/en/view/109749255/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1604: All versions < V2.7	Update to V2.8.0 https://support.industry.siemens.com/cs/ww/en/view/109762689/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1616: All versions < V2.7	Update to V2.8.0 https://support.industry.siemens.com/cs/ww/en/view/109762689/ See further recommendations from section Workarounds and Mitigations
SIMATIC DK-16xx PN IO: All versions < V2.7	Update to V2.8.0 https://support.industry.siemens.com/cs/ww/en/view/109762689/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200AL: All versions < V1.0.2	Update to V1.0.2 https://support.industry.siemens.com/cs/ww/en/view/109479281/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 4AO U/I 4xM12 (6ES7145-6HD00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8 DIO, DC24V/1,3A, 8xM12 (6ES7147-6BG00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8 DO, DC24V/2A, 8xM12 (6ES7142-6BR00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8AI RTD/TC 8xM12 (6ES7144-6KD50-0AB0): All versions	Currently no remediation 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 remediation is planned See recommendations from section Workarounds and Mitigations

SIMATIC ET200ecoPN, 8DI, DC24V, 4xM12 (6ES7141-6BF00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DI, DC24V, 8xM12 (6ES7141-6BG00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/0,5A, 4xM12 (6ES7142-6BF50-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 4xM12 (6ES7142-6BF00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 8xM12 (6ES7142-6BG00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 16DI, DC24V, 8xM12 (6ES7141-6BH00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN, 16DO DC24V/1,3A, 8xM12 (6ES7142-6BH00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200ecoPN: IO-Link Master (6ES7148-6JA00-0AB0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200M (incl. SIPLUS variants): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200MP IM155-5 PN BA (incl. SIPLUS variants): All versions < V4.0.1	Update to V4.0.1 or newer 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 < V4.2	Update to V4.2 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 < V4.1	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/78647504/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET200pro: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations

SIMATIC ET200S (incl. SIPLUS variants): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP (incl. SIPLUS variants, except IM155-6 PN ST and IM155-6 PN HF): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants): All versions < 4.2.0	Update to V4.2.0 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 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 < V4.1.0	Update to V4.1.0 https://support.industry.siemens.com/cs/de/de/view/78648144/ See further recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort Panels, HMI Multi Panels, HMI Mobile Panels (incl. SIPLUS variants): All versions < V15.1	Update to V15.1 https://support.industry.siemens.com/cs/ww/en/view/109761576/ See further recommendations from section Workarounds and Mitigations
SIMATIC MV400 family: All Versions < V7.0.6	Update to V7.0.6 https://support.industry.siemens.com/cs/ww/en/view/109793481/ See further recommendations from section Workarounds and Mitigations
SIMATIC PN/PN Coupler (incl. SIPLUS NET variants): All versions < V4.0	Upgrade to V4.0 https://support.industry.siemens.com/cs/ww/en/view/109749637/ See further recommendations from section Workarounds and Mitigations
SIMATIC RF650R: All versions < V3.0	Update to V3.0 https://support.industry.siemens.com/cs/ww/en/view/109743740/ See further recommendations from section Workarounds and Mitigations
SIMATIC RF680R: All versions < V3.0	Update to V3.0 https://support.industry.siemens.com/cs/ww/en/view/109743740/ See further recommendations from section Workarounds and Mitigations
SIMATIC RF685R: All versions < V3.0	Update to V3.0 https://support.industry.siemens.com/cs/ww/en/view/109743740/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-200 SMART: All versions < V2.3	Contact your local Siemens representative or the Siemens customer support at https://w3.siemens.com/aspa_app/ to receive firmware version 2.3. Update to V2.3 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V3.X.14	Update to V3.X.14 https://support.industry.siemens.com/cs/ww/en/ps/13752/dl See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H 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/109474550/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V6 CPU family (incl. SIPLUS variants): All versions < V6.0.6	Update to V6.0.6 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	Update to V7.0.2 https://support.industry.siemens.com/cs/ww/en/view/109752685/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-410 CPU family (incl. SIPLUS variants): All versions < V8.2	Update to V8.2 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 < V4.2.1	Update to V4.2.1 https://support.industry.siemens.com/cs/ww/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 < V2.1	Update to V2.1 https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller (incl. F): All versions < V2.1	Update to V2.1 https://support.industry.siemens.com/cs/ww/en/view/109478528/ See further recommendations from section Workarounds and Mitigations
SIMATIC TDC CP51M1: All versions < V1.1.8	Update to V1.1.8 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	Update to V1.1.1 https://support.industry.siemens.com/cs/ww/en/view/109740119/ See further recommendations from section Workarounds and Mitigations
SIMATIC Teleservice Adapter IE Advanced: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC Teleservice Adapter IE Basic: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC Teleservice Adapter IE Standard: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
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/ See further recommendations from section Workarounds and Mitigations
SIMOCODE pro V PN (incl. SIPLUS variants): All versions < V2.0.0	Update to V2.0.0 https://support.industry.siemens.com/cs/ww/en/view/109749989/ See further recommendations from section Workarounds and Mitigations
SIMOTION (incl. SIPLUS variants): All versions < V4.5 HF1	Update to V4.5 HF1 https://support.industry.siemens.com/cs/ww/en/view/109742328/ See further recommendations from section Workarounds and Mitigations
SINAMICS DCM w. PN: All versions < V1.4 SP1 HF5	Update to V1.4 SP1 HF5 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 HF1	Update to V1.2 HF1 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 SP6 HF3	Update to V4.7 SP6 HF3 https://support.industry.siemens.com/cs/ww/en/view/109482659/ See further recommendations from section Workarounds and Mitigations
SINAMICS G120(C/P/D) w. PN (incl. SIPLUS variants): All versions < V4.7 SP6 HF3	Update to V4.7 SP6 HF3 https://support.industry.siemens.com/cs/ww/en/view/109482659/ See further recommendations from section Workarounds and Mitigations

SINAMICS G130 V4.7 w. PN: All versions < V4.7 HF27	Update to V4.7 HF27 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	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: V4.7: All versions < V4.7 HF27	Update to V4.7 HF27 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	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 HF5	Update V4.4 SP3 HF5 https://support.industry.siemens.com/cs/ww/en/view/109474320/ See further recommendations from section Workarounds and Mitigations
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/ww/en/view/109758423/ See further recommendations from section Workarounds and Mitigations
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/ww/en/view/109758423/ See further recommendations from section Workarounds and Mitigations
SINAMICS S120 V4.7 w. PN (incl. SIPLUS variants): All versions < V4.7 HF27	Update to V4.7 HF27 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 HF4	Update to V4.8 HF4 https://support.industry.siemens.com/cs/ww/en/view/109740193/ See further recommendations from section Workarounds and Mitigations
SINAMICS S150 V4.7 w. PN: All versions < V4.7 HF27	Update to V4.7 HF27 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	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 < V1.01	Update to V1.01 https://support.industry.siemens.com/cs/ww/en/view/109746210/ See further recommendations from section Workarounds and Mitigations
SINUMERIK 828D V4.5 and prior: All versions < V4.5 SP6 HF2	Update to V4.5 SP6 HF2 SINUMERIK software can be obtained from your local Siemens account manager See further recommendations from section Workarounds and Mitigations
SINUMERIK 828D V4.7: All versions < V4.7 SP4 HF1	Update to V4.7 SP4 HF1. SINUMERIK software can be obtained from your local Siemens account manager See further recommendations from section Workarounds and Mitigations
SINUMERIK 840D sl V4.5 and prior: All versions < V4.5 SP6 HF2	Update to V4.5 SP6 HF2 SINUMERIK software can be obtained from your local Siemens account manager See further recommendations from section Workarounds and Mitigations
SINUMERIK 840D sl V4.7: All versions < V4.7 SP4 HF1	Update to V4.7 SP4 HF1 SINUMERIK software can be obtained from your local Siemens account manager See further recommendations from section Workarounds and Mitigations
SIRIUS ACT 3SU1 interface module PROFINET: All versions < V1.1.0	Update to V1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109753683/ See further recommendations from section Workarounds and Mitigations
SIRIUS Motor Starter M200D PROFINET: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIRIUS Soft Starter 3RW44 PN: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SITOP PSU8600 PROFINET: All versions < V1.2.0	Update to V1.2.0 https://support.industry.siemens.com/cs/ww/en/view/102295547/ See further recommendations from section Workarounds and Mitigations
SITOP UPS1600 PROFINET (incl. SIPLUS variants): All versions < V2.2.0	Update to V2.2.0 https://support.industry.siemens.com/cs/ww/en/view/79207181/ See further recommendations from section Workarounds and Mitigations

Softnet PROFINET IO for PC-based Windows systems: All versions < V14 SP1	Upgrade to V14 SP1 https://support.industry.siemens.com/cs/ww/en/view/109747482/ 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:

- Apply cell protection concept: https://www.siemens.com/cert/operational-guidelines-industrial-security.
- Use VPN for protecting network communication between cells.
- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security.
- For SIMATIC Teleservice Adapters (IE Basic, IE Standard, IE Advanced): migrate to a successor product within the SCALANCE M-800 family. For details refer to the notice of discontinuation.

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

IE/PB-Link devices enable existing PROFIBUS devices to be integrated into a PROFINET application.

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

SCALANCE W-700 products are wireless communication devices based on IEEE 802.11 standards. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

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

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

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 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 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 (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.

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.

SIRIUS ACT is a modular system of pushbuttons and indicator lights for front plate mounting and rear-mounted electrical modules.

SIRIUS M200D motor starters for distributed installation start, monitor and protect motors and loads up to 5.5 kW.

SITOP UPS1600 devices augment DC 24V power supply units to offer uninterruptible rated currents up to 40A from battery modules.

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

TeleControl Server Basic allows remote monitoring and control of plants.

The Development Kit DK-16xx PN IO permits an easy integration of CP 1616 and CP 1604 in non-Windows operating system environments.

The IE/AS-i LINK PN IO is a compact network transition between PROFINET/Industrial Ethernet (PROFINET IO-Device) and AS-Interface.

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

The SCALANCE M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

The SIMATIC CM 1542-1 communication module is used to connect S7-1500 controllers to PROFINET as IO-Controller.

The SIMATIC CP 1243-1 communication processor connects the S7-1200 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC CP 1616 and CP 1604 interface cards are used for connecting Personal Computers and PCI-104 systems to PROFINET IO.

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

The SITOP PSU8600 expandable power supply system is connected to a 3-phase AC line supply to offer regulated DC power.

The stationary optical readers of the SIMATIC MV400 family are used to reliably capture printed, lasered, drilled, punched and dotpeen codes on a variety of different surfaces.

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-2017-2680

Specially crafted PROFINET DCP broadcast packets could cause a denial of service condition of affected products on a local Ethernet segment (Layer 2). Human interaction is required to recover the systems. PROFIBUS interfaces are not affected.

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-400: Uncontrolled Resource Consumption

Vulnerability CVE-2017-2681

Specially crafted PROFINET DCP packets sent on a local Ethernet segment (Layer 2) to an affected product could cause a denial of service condition of that product. Human interaction is required to recover the system. PROFIBUS interfaces are not affected. This vulnerability affects only SIMATIC HMI Multi Panels and HMI Mobile Panels, and S7-300/S7-400 devices.

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-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
- Duan JinTong, Ma ShaoShuai, and Cheng Lei from NSFOCUS Security Team for coordinated disclosure
- CNCERT/CC for coordination efforts

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 (2017-05-08): Publication Date

V1.1 (2017-06-13): Added update information for SALANCE X-300/X408, X414, SITOP PSU8600/ UPS 1600 PROFINET and S7-400

V1.2 (2017-07-21): Added update information for SCALANCE XM-400, SCALANCE XR-500, SIMATIC S7-400-H V6, SINAMICS S110, SINAMICS S120 and SINAMICS V90

V1.3 (2017-08-16): Added update information for SIMATIC CP 1542SP-1, CP 1542SP-1 IRC, and CP 1543SP-1, SIMATIC ET 200SP, SIMATIC S7-200 SMART, SINAMICS G130, G150, and S150, and SINUMERIK 828D; Adjusted update information for Development/Evaluation Kits

V1.4 (2017-09-13): Added update information for SCALANCE M-800 / S615

V1.5 (2017-10-09): Detailed SIMATIC CP 1243-1, Added update information for SIMATIC CP 1243-1, 1243-1 IRC, SINAMICS DCM and added upgrade information for PN/PN Coupler

V1.6 (2017-11-09): Added upgrade and update information for Softnet PROFINET IO and SIMATC ET 200AL

V1.7 (2017-11-23): Added update information for SCALANCE X-200 and SIMATIC S7-400 PN/DP V6 Incl. F

V1.8 (2018-01-18): New advisory format, added update information for SIMOCODE pro V PROFINET

V1.9 (2018-01-24): Corrected information for SIMATIC CM 1542-1 and ET 200MP. Added solution for SINAMICS DCP, and S7-400 V7 PN/DP

V2.0 (2018-02-22): Refined ET 200MP product family; Added update information for ET 200MP IM155-5 PN ST

V2.1 (2018-03-06): Added update information for SCALANCE X-200IRT

V2.2 (2018-05-03): Added update information for SIMATIC CP 343-1 Std and CP 343-1 Lean

V2.3 (2018-11-13): Updated information for SINAMICS S120, SIMATIC ET 200SP (except IM155-6 PN ST), SIMATIC Panels

V2.4 (2018-12-11): Updated information for SIMATIC ET 200MP IM155-5 PN HF, SIRIUS ACT 3SU1 interface module PROFINET

V2.5 (2018-12-13): Corrected download links, update for CP 1243-1 not available, see mitigations

V2.6 (2019-01-08): Updated information for CP 1243-1

V2.7 (2019-10-08): Renamed SIMATIC WinAC RTX 2010 incl. F to SIMATIC WinAC RTX (F) 2010 and updated information for SIMATIC WinAC RTX (F) 2010

V2.8 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

V2.9 (2020-07-14): Added SIMATIC TDC CP51M1 and CPU555 to the list of affected products

V3.0 (2020-08-11): Informed about successor product for SIMATIC Teleservice adapters. Added SIMATIC ET200ecoPN product variants (MLFB IDs) that are not affected

V3.1 (2021-03-09): Added ecoPN model (6ES7148-6JG00-0BB0) as not affected. Added MV400 and update information. Updated CWE classification for CVE-2017-2680 and CVE-2017-2681

V3.2 (2021-06-08): Consolidated product names and added SIMATIC ET200SP IM155-6 PN HS to the advisory

V3.3 (2021-10-12): Clarified product name for SIMATIC NET CP 443-1 OPC UA and clarified affected ET200ecoPN models

V3.4 (2022-02-08): No remediation planned for SIMATIC CP 443-1 OPC UA; added more information to the advisory title; no remediation planned for ET200 devices

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through 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.