SSA-780073: Denial-of-Service Vulnerability in PROFINET Devices via DCE-RPC Packets

Publication Date: 2020-02-11
Last Update: 2020-02-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

Products that include the Siemens PROFINET-IO (PNIO) stack in versions prior V06.00 are potentially affected by a denial-of-service vulnerability when multiple legitimate diagnostic package requests are sent to the DCE-RPC interface.

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.

Additionally, Siemens recommends other vendors of PROFINET devices to check if their products have incorporated a vulnerable version of the Siemens PNIO stack as part of the Siemens Development/Evaluation Kits.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller: All versions	See recommendations from section Workarounds and Mitigations
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All Versions < V4.5	Update to V4.5 Patch 01 https://support.industry.siemens.com/cs/ww/en/view/109760397/
Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All Versions < V4.6	Update to V4.6 https://support.industry.siemens.com/cs/ww/en/view/109765183/
PROFINET Driver for Controller: All Versions < V2.1	Update to V2.1 Patch 03 https://support.industry.siemens.com/cs/ww/en/view/109768047/
RUGGEDCOM RM1224: All versions < V4.3	See SCALANCE M-800 / S615
SCALANCE M-800 / S615: All versions < V4.3	Update to V6.1.2 https://support.industry.siemens.com/cs/ww/en/view/109772130/
SCALANCE W700 IEEE 802.11n: All versions <= V6.0.1	Update to V6.4 https://support.industry.siemens.com/cs/ww/en/view/109773308/

SCALANCE X-200 switch family (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE X-200IRT switch family (incl. SIPLUS NET variants): All Versions < V5.3	Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309/
SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SCALANCE XB-200, XC-200, XP-200, XF-200BA and XR-300WG: All Versions < V3.0	Update to V4.1 https://support.industry.siemens.com/cs/ww/en/view/109762982/
SCALANCE XM-400 switch family: All Versions < V6.0	Update to V6.2.3 https://support.industry.siemens.com/cs/ww/en/view/109771191/
SCALANCE XR-500 switch family: All Versions < V6.0	Update to V6.2.3 https://support.industry.siemens.com/cs/ww/en/view/109771193/
SIMATIC CP 1616 and CP 1604: All Versions < V2.8	Update to V2.8.1 https://support.industry.siemens.com/cs/ww/en/view/109768663/
SIMATIC CP 343-1 (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Advanced (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 ERPC: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 LEAN (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced (incl. SIPLUS NET variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 OPC UA: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200AL IM 157-1 PN: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC ET200M IM153-4 PN IO HF (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200M IM153-4 PN IO ST (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants): All Versions < V4.2.0	Update to V4.2.0 https://support.industry.siemens.com/cs/ww/en/view/93012181/
SIMATIC ET200MP IM155-5 PN ST (incl. SIPLUS variants): All Versions < V4.1.0	Update to V4.1.0 https://support.industry.siemens.com/cs/ww/en/view/78647504/
SIMATIC ET200S (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN Basic (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants): All Versions < V3.3.1	Update to V4.2.2 https://support.industry.siemens.com/cs/ww/en/view/85624387/
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/ww/en/view/78648144/
SIMATIC ET200ecoPN (except 6ES7148-6JD00-0AB0 and 6ES7146-6FF00-0AB0): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200pro, IM 154-3 PN HF: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200pro, IM 154-4 PN HF: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC Support, Package for VxWorks: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC MV400 family: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PN/PN Coupler 6ES7158-3AD01-0XA0 (incl. SIPLUS NET variant): All Versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF180C: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC RF182C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF600 family: All versions < V3	Update to V3.2.1 https://support.industry.siemens.com/cs/ww/en/view/109768501
SINAMICS DCP: All Versions < V1.3	Update to V1.3 https://support.industry.siemens.com/cs/ww/en/view/109773826/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- If possible, disable PROFINET
- SCALANCE M-800 / S615 and RUGGEDCOM RM1224: Create a firewall rule that blocks the PROFINET Context Manager port (34964/udp)

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

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

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

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

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

The SCALANCE M 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.

SCALANCE W products are wireless communication devices used to connect industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs), according to the IEEE 802.11 standard (802.11ac, 802.11a/b/g/h, and/or 802.11n).

CP 1616 and CP 1604 are PCI/PCI-104 cards for high-performance connection of field devices to Industrial Ethernet with PROFINET.

Communication Processor (CP) modules of families SIMATIC CP 343-1 and CP 443-1 have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet communication.

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 RF180C is an RFID communication module for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet. The SIMATIC RF180C is designed for use in PROFINET networks and is integrated in SIMATIC STEP 7 via the GSDML file.

SIMATIC RF182C is an RFID communication module for direct connection of SIMATIC identification systems to Ethernet/IP. The SIMATIC RF182C is designed for use in Ethernet networks based on TCP/IP and communicates via XML.

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.

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

With the SIMATIC IPC Support Package for VxWorks, Siemens offers support for industrial computers (SIMATIC IPCs) for the VxWorks real-time operating system.

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

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-2019-13946

Profinet-IO (PNIO) stack versions prior V06.00 do not properly limit internal resource allocation when multiple legitimate diagnostic package requests are sent to the DCE-RPC interface. This could lead to a denial of service condition due to lack of memory for devices that include a vulnerable version of the stack.

The security vulnerability could be exploited by an attacker with network access to an affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device.

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 ('Resource Exhaustion')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Yuval Ardon and Matan Dobrushin from OTORIO for coordinated disclosure

- The Cybersecurity and Infrastructure Security Agency (CISA) 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 (2020-02-11): Publication Date

TERMS OF USE