SSA-978220: Denial-of-Service Vulnerability over SNMP in Multiple Industrial Products

Publication Date: 2020-02-11
Last Update: 2020-08-11
Current Version: V1.2
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 to update to the new versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
IE/PB LINK PN IO (incl. SIPLUS NET variants): All versions < V4.0.1	Update to V4.0.1 https://support.industry.siemens.com/cs/ww/en/view/109780330/
SCALANCE S602: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE S612: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE S623: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE S627-2M: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1623: All versions < V14.00.15.00_51.25.00.01	Update to SIMATIC NET PC Software V16 https://support.industry.siemens.com/cs/ww/en/view/109775589
SIMATIC NET CP 1626: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1628: All versions < V14.00.15.00_51.25.00.01	Update to SIMATIC NET PC Software V16 https://support.industry.siemens.com/cs/ww/en/view/109775589
SIMATIC NET CP 343-1 Advanced (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 443-1 (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations

SIMATIC NET CP 443-1 Advanced (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 443-1 OPC UA: All versions	See recommendations from section Workarounds and Mitigations
TIM 1531 IRC (incl. SIPLUS NET variants): All versions < V2.0	Update to V2.0 https://support.industry.siemens.com/cs/ww/en/view/109774204

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.
- For SCALANCE S-600 family (S602, S612, S623, S627-2M): migrate to a successor product within the SCALANCE SC-600 family, V2.1 or later version. 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

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN networks.

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

SIMATIC NET CP 1623 and CP 1628 are PCI express cards for connection to Industrial Ethernet.

SIMATIC NET CP 1626 enables SIMATIC PGs/PCs and PCs equipped with a PCI Express slot to be connected to PROFINET IO.

The SCALANCE S-600 devices (S602, S612, S623, S627-2M) are used to protect trusted industrial networks from untrusted networks. The S-600 devices are superseded by the SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C), or the SCALANCE S615.

The SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

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-2015-5621

An error in the message handling of SNMP messages allows remote attackers to cause a Denial-of-Service (DoS) and possibly execute arbitrary code via a crafted packet sent on port 161/udp (SNMP).

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

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:W/RC:C
CWE	CWE-19: Data Processing Errors

Vulnerability CVE-2018-18065

A NULL Pointer Exception bug within the SMNP handling code allows authenticated attacker to remotely cause a Denial-of-Service (DoS) via a crafted packet sent on port 161/udp (SNMP).

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

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky Lab for coordinated disclosure

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
V1.1 (2020-07-14): Added solution for IE/PB LINK PN IO
V1.2 (2020-08-11): Informed about successor products for the SCALANCE S-600 family

TERMS OF USE