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

Publication Date: 2020-02-11
Last Update: 2023-04-11
Current Version: V1.8
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 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 latest versions. Siemens 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 (6GK1411-5AB10):<br>All versions < V4.0.1 | Update to V4.0.1 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109780330/<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE S602:<br>All versions < V4.1 | Update to V4.1<br>Update is only available via Siemens Support contact<br><br>Migrate to a successor product within the SCALANCE SC-600 family, V2.1 (https://support.industry.siemens.com/cs/ww/en/view/109780500) or later version<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE S612:<br>All versions < V4.1 | Update to V4.1<br>Update is only available via Siemens Support contact<br><br>Migrate to a successor product within the SCALANCE SC-600 family, V2.1 (https://support.industry.siemens.com/cs/ww/en/view/109780500) or later version<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE S623:<br>All versions < V4.1 | Update to V4.1<br>Update is only available via Siemens Support contact<br><br>Migrate to a successor product within the SCALANCE SC-600 family, V2.1 (https://support.industry.siemens.com/cs/ww/en/view/109780500) or later version<br>See further recommendations from section Workarounds and Mitigations |
| SCALANCE S627-2M:<br>All versions < V4.1 | Update to V4.1<br>Update is only available via Siemens Support Contact<br><br>Migrate to a successor product within the SCALANCE SC-600 family, V2.1 (https://support.industry.siemens.com/cs/ww/en/view/109780500) or later version<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC CP 443-1 (6GK7443-1EX30-0XE0):<br>All versions < V3.3 | Update to V3.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109817938/<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC CP 443-1 (6GK7443-1EX30-0XE1):<br>All versions < V3.3 | Update to V3.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109817938/<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0):<br>All versions < V3.3 | Update to V3.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109817938/<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC CP 443-1 OPC UA (6GK7443-1UX00-0XE0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC CP 1623 (6GK1162-3AA00):<br>All versions < V14.00.15.00_51.25.00.01 | The updated firmware is contained in SIMATIC NET PC Software V14 Update 14 or later version or SIMATIC NET PC Software V16 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109775589/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC CP 1626 (6GK1162-6AA01):<br>All versions < V1.1.1 | Update to V1.1.1 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109792924/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC CP 1628 (6GK1162-8AA00):<br>All versions < V14.00.15.00_51.25.00.01 | Update to SIMATIC NET PC Software V16 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109775589/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS NET CP 443-1 (6AG1443-1EX30-4XE0):<br>All versions < V3.3 | Update to V3.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109817938/<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0):<br>All versions < V3.3 | Update to V3.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109817938/<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS NET IE/PB link PN IO (6AG1411-5AB10-2AA0):<br>All versions < V4.0.1 | Update to V4.0.1 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109780330/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0):<br>All versions < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109774204/<br>See further recommendations from section Workarounds and Mitigations |
| TIM 1531 IRC (6GK7543-1MX00-0XE0):<br>All versions < V2.0 | Update to V2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109774204/<br>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:

- Disable SNMP if supported by the product; disabling SNMP fully mitigates the vulnerability
- Protect network access to port 161/udp of affected devices
- Use VPN for protecting network communication between cells

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

SIMATIC CP 1623, CP 1626 and CP 1628 are PCI express cards for connection to Industrial Ethernet.

IE/PB link PN IO is a gateway between Industrial Ethernet and PROFIBUS.

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.

SIMATIC CP 343-1 and CP 443-1 are communication processors (CP) designed to enable Ethernet communication for SIMATIC S7-300/S7-400 CPUs.

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.

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.

## 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 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:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2018-18065

A NULL Pointer Exception bug within the SMNP handling code allows authenticated attacker to remotely cause a denial of service 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 party for its efforts:

- Artem Zinenko from Kaspersky Lab for coordinated disclosure

## ADDITIONAL INFORMATION

For SCALANCE S-600 family (S602, S612, S623, S627-2M): migrate to a successor product within the SCALANCE SC-600 family, V2.1 (https://support.industry.siemens.com/cs/ww/en/view/109780500) or later version. For details refer to the notice of discontinuation (https://support.industry.siemens.com/cs/ww/en/view/109756957).

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 |
| V1.3 (2021-02-09): | Added solution for SIMATIC NET CP 1626 |
| V1.4 (2021-04-13): | Added solution for SCALANCE S602, SCALANCE S612, SCALANCE S623, and SCALANCE S627-2M |
| V1.5 (2022-02-08): | No remediation planned for SIMATIC CP 443-1 OPC UA, SIMATIC CP 343-1 Advanced, SIPLUS NET CP 343-1 Advanced |
| V1.6 (2022-04-12): | Updated remediation for SIMATIC CP 1623 |
| V1.7 (2022-06-14): | No fix planned for SIMATIC CP 343-1 Advanced |
| V1.8 (2023-04-11): | Added fix for SIMATIC CP 443-1 and CP 443-1 Advanced |

## TERMS OF USE