# SSA-635129: Denial-of-Service Vulnerabilities in EN100 Ethernet Communication Module and SIPROTEC 5 relays

Publication Date: 2018-07-11
Last Update: 2018-07-11
Current Version: V1.0
CVSS v3.0 Base Score: 7.5

## SUMMARY

The EN100 Ethernet communication module and SIPROTEC 5 relays are affected by security vulnerabilities which could allow an attacker to conduct a Denial-of-Service attack over the network.

Siemens has released updates for several affected products, is working on updates for the remaining affected products, and recommends specific countermeasures until fixes are available.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Firmware variant IEC 61850 for EN100 Ethernet module:<br>All versions < V4.33 | Update to V4.33<br>https://support.industry.siemens.com/cs/us/en/view/109745821 |
| Firmware variant PROFINET IO for EN100 Ethernet module:<br>All versions | See recommendations from section Workarounds and Mitigations |
| Firmware variant Modbus TCP for EN100 Ethernet module:<br>All versions | See recommendations from section Workarounds and Mitigations |
| Firmware variant DNP3 TCP for EN100 Ethernet module:<br>All versions | See recommendations from section Workarounds and Mitigations |
| Firmware variant IEC104 for EN100 Ethernet module:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIPROTEC 5 relays with CPU variants CP300 and CP100 and the respective Ethernet communication modules:<br>All versions < V7.80<br>only affected by CVE-2018-11451 | Update to firmware version V7.80 for the following device types: 6MD85, 6MD86, 7SS85, 7KE85, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, and 7UT87.<br>Search for “SIPROTEC 5 <Device type> - DIGSI Device Drivers V7.8x” under https://support.industry.siemens.com/. The firmware version V7.80 for the communications modules can also be found on each device specific download page: See under “Additional DIGSI Device Driver > Protocols”. |

  

| | |
|---|---|
| SIPROTEC 5 relays with CPU variants CP200 and the respective Ethernet communication modules:<br>All versions<br>only affected by CVE-2018-11451 | 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:

- Block access to port 102/tcp e.g. with an external firewall.

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

Recommended security guidelines to Secure Substations can be found at:

https://www.siemens.com/gridsecurity

## PRODUCT DESCRIPTION

The EN100 Ethernet modules are used for enabling process communication on either IEC 61850, PROFINET IO, Modbus TCP, DNP3 TCP or IEC 104 protocols via electrical/optical 100 Mbit interfaces on SIPROTEC 4, SIPROTEC Compact and Reyrolle devices.

SIPROTEC 5 devices provide a wide range of integrated protection, control, measurement, and automation functions for electrical substations and other fields of application.

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

### Vulnerability CVE-2018-11451

Specially crafted packets to port 102/tcp could cause a denial-of-service condition in the affected products. A manual restart is required to recover the EN100 module functionality of SIPROTEC 4 and SIPROTEC Compact relays.

Successful exploitation requires an attacker with network access to send multiple packets to the affected products or modules. As a precondition the IEC 61850-MMS communication needs to be activated on the affected products or modules. No user interaction or privileges are required to exploit the vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the network functionality of the device, compromising the availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

| | |
|---|---|
| CVSS v3.0 Base Score | 7.5 |
| CVSS Vector | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |

Vulnerability CVE-2018-11452

Specially crafted packets to port 102/tcp could cause a denial-of-service condition in the EN100 communication module if oscillographs are running. A manual restart is required to recover the EN100 module functionality.

Successful exploitation requires an attacker with network access to send multiple packets to the EN100 module. As a precondition the IEC 61850-MMS communication needs to be activated on the affected EN100 modules. No user interaction or privileges are required to exploit the security vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the network functionality of the device, compromising the availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

| | |
|---|---|
| CVSS v3.0 Base Score | 5.9 |
| CVSS Vector | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Victor Nikitin, Vladislav Suchkov, and Ilya Karpov from ScadaX 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 (2018-07-11): Publication Date

## TERMS OF USE