SSA-845879: Firmware Downgrade Vulnerability in EN100 Ethernet Communication Module for SIPROTEC 4, SIPROTEC Compact and Reyrolle

Publication Date: 2018-03-08
Last Update: 2019-02-12
Current Version: V1.2
CVSS v3.0 Base Score: 7.5

SUMMARY

The EN100 Ethernet communication module, which is an optional extension for SIPROTEC 4, SIPRO-TEC Compact and Reyrolle devices, allows an unauthenticated upload of firmware updates to the communication module in affected versions.

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

SIPROTEC 4, SIPROTEC Compact and Reyrolle devices can be extended with an EN100 module.

For customers who are currently using the discontinued EN100-E or EN100-O modules, Siemens recommends to upgrade to EN100-E+ or EN100-O+ modules in order to apply the firmware updates.

Affected Product and Versions	Remediation
EN100 Ethernet module IEC 61850 variant: All versions < V4.30	Update to V4.30 and configure maintenance password https://support.industry.siemens.com/cs/us/en/view/109745821
EN100 Ethernet module DNP3 variant: All versions < V1.04	Update to V1.04 and configure maintenance password https://support.industry.siemens.com/cs/us/en/view/109745821
EN100 Ethernet module PROFINET IO variant: All versions	See recommendations from section Workarounds and Mitigations
EN100 Ethernet module Modbus TCP variant: All versions	See recommendations from section Workarounds and Mitigations
EN100 Ethernet module IEC 104 variant: All versions < V1.22	Update to V1.22 and configure maintenance password https://support.industry.siemens.com/cs/document/109745821

WORKAROUNDS AND MITIGATIONS

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

- Apply secure substation concept and Defense-in-Depth (see https://www.siemens.com/gridsecurity)

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.

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-2018-4838

The web interface (TCP/80) of affected devices allows an unauthenticated user to upgrade or down-grade the firmware of the device, including to older versions with known vulnerabilities.

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:H/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Ilya Karpov and Alexey Stennikov from Positive Technologies for coordinated disclosure

ADDITIONAL INFORMATION

For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2018-03-08):	Publication Date
V1.1 (2018-04-17):	Added update for DNP3 TCP
V1.2 (2019-02-12):	Added update information for IEC 104 variant of EN100 module

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.