SSA-418979: Vulnerabilities in EN100 Ethernet Communication Module

Publication Date: 2019-12-10
Last Update: 2020-01-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

The EN100 Ethernet communication modules are affected by security vulnerabilities which could allow an attacker to disclose information. 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
EN100 Ethernet module IEC 61850 variant: All versions < V4.37	Update to V4.37 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 DNP3 variant: All versions	See recommendations from section Workarounds and Mitigations
EN100 Ethernet module IEC104 variant: All versions	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 80/tcp and 443/tcp e.g. with an external firewall.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

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, Reyrolle and SWT3000 devices.

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-2019-13942

An unauthorized user could exploit a buffer overflow vulnerability in the webserver. Specially crafted packets sent could cause a Denial-of-Service condition and if certain conditions are met, the affected devices must be restarted manually to fully recover.

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

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2019-13943

The web interface could allow Cross-Site Scripting (XSS) attacks if an attacker is able to modify content of particular web pages, causing the application to behave in unexpected ways for legitimate users. Successful exploitation does not require for an attacker to be authenticated to the web interface. This could allow the attacker to read or modify contents of the web application.

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

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2019-13944

A vulnerability in the integrated web server of the affected devices could allow unauthorized attackers to obtain sensitive information about the device, including logs and configurations.

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

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-23: Relative Path Traversal

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 (2019-12-10):	Publication Date
V1.1 (2020-01-14):	Included SWT3000 in the product description section

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.