SSA-693555: Memory Corruption Vulnerability in EN100 Ethernet Module

Publication Date: 2022-06-14
Last Update: 2022-06-14
Current Version: V1.0
CVSS v3.1 Base Score: 8.6

SUMMARY

EN100 Ethernet module is affected by memory corruption vulnerability (CVE-2022-30937).

Siemens has released an update for the EN100 Ethernet module IEC 61850 variant and recommends to update to the latest version. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
EN100 Ethernet module DNP3 IP variant: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
EN100 Ethernet module IEC 104 variant: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
EN100 Ethernet module IEC 61850 variant: All versions < V4.37	Update to V4.37 or later version https://support.industry.siemens.com/cs/us/en/view/109745821/ See further recommendations from section Workarounds and Mitigations
EN100 Ethernet module Modbus TCP variant: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
EN100 Ethernet module PROFINET IO variant: All versions	Currently no fix is planned 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:

- Disable web service within the device configuration if it is not used
- Block access to port 80/tcp and 443/tcp e.g. with an external firewall
- Apply secure substation concept and Defense-in-Depth (see https://www.siemens.com/gridsecurity) or contact customer care to find specific solutions

Product specific remediations or mitigations can be found in the section Affected Products and Solution.

Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) 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 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 IP 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-2022-30937

Affected applications contains a memory corruption vulnerability while parsing specially crafted HTTP packets to /txtrace endpoint. This could allow an attacker to crash the affected application leading to a denial of service condition.

CVSS v3.1 Base Score	8.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Messner from Siemens Energy for reporting the vulnerabilities

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 (2022-06-14):	Publication Date

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.