SSA-845392: Multiple Vulnerabilities in Nucleus RTOS based Siemens Energy PLUSCONTROL 1st Gen Devices

Publication Date:	2022-01-11
Last Update:	2022-01-11
Current Version:	V1.0
CVSS v3.1 Base Score:	8.2

SUMMARY

Multiple vulnerabilities (also known as “NUCLEUS:13”) have been identified in the Nucleus RTOS (real-time operating system) and reported in the Siemens Security Advisory SSA-044112: https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf.

PLUSCONTROL 1st Gen devices are affected by some of the vulnerabilities as documented below.

Siemens Energy recommends specific countermeasures for products where updates are not available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
PLUSCONTROL 1st Gen: All versions	Currently no remediation 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:

- PLUSCONTROL devices are typically located in a separate LAN segment of energy transmission solutions, where an attacker could use these vulnerabilities to disrupt SER messages or Trace functionalities. Therefore, review the status of the defense in depth recommendations that apply to your specific deployment and align as needed. Especially the measures on the network layer to prevent accessibility from other network segments.

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 Energy 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 Energy 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 Energy 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.

PRODUCT DESCRIPTION

PLUSCONTROL products from Siemens Energy are control devices for high power energy transmission with modular multilevel converters.

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-2021-31344

ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004)

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

Vulnerability CVE-2021-31345

The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006)

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-1284: Improper Validation of Specified Quantity in Input

Vulnerability CVE-2021-31346

The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007)

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-1284: Improper Validation of Specified Quantity in Input

Vulnerability CVE-2021-31885

TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009)

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-805: Buffer Access with Incorrect Length Value

Vulnerability CVE-2021-31889

Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015)

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-191: Integer Underflow (Wrap or Wraparound)

Vulnerability CVE-2021-31890

The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017)

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-240: Improper Handling of Inconsistent Structural Elements

ADDITIONAL INFORMATION

Products listed in this advisory use the Nucleus RTOS (Real-time operating system).

For more details regarding the vulnerabilities reported for Nucleus RTOS refer to Siemens Security Advisory SSA-044112: https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf

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 (2022-01-11): 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.