SSA-223353: Multiple Vulnerabilities in Nucleus RTOS based SIMOTICS CONNECT 400

Publication Date: 2022-03-08
Last Update: 2022-03-08
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), originally reported in the Siemens Security Advisory SSA-044112: https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf.

SIMOTICS CONNECT 400 devices are affected by some of the vulnerabilities as documented below.

Siemens has released an update for the SIMOTICS CONNECT 400 and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMOTICS CONNECT 400: All versions < V0.5.0.0	Update to V0.5.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109778383/
SIMOTICS CONNECT 400: All versions < V1.0.0.0 only affected by CVE-2021-31344, CVE-2021-31346, CVE-2021-31890	Update to V1.0.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109778383/

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

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

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

SIMOTICS CONNECT 400 is a connector and sensor box, mounted on low-voltage motors to provide analytics data for the MindSphere application SIDRIVE IQ Fleet.

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-2021-31346

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-2021-31889

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 (2022-03-08): Publication Date

TERMS OF USE