SSA-044112: Multiple Vulnerabilities (NUCLEUS:13) in the TCP/IP Stack of Nucleus RTOS

Publication Date: 2021-11-09
Last Update: 2021-12-14
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

The TCP/IP stack and related services (FTP, TFTP) of the networking component (Nucleus NET) in Nucleus Real-Time Operating System (RTOS) contain several vulnerabilities, also known as “NUCLEUS:13” and as documented below.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends countermeasures for products where updates are not available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Nucleus NET: All versions	Currently no remediation is planned Update to the latest version of Nucleus ReadyStart V3 or V4 Contact customer support or your local Nucleus Sales team for mitigation advice
Nucleus ReadyStart V3: All versions < V2017.02.4	Update to V2017.02.4 or later version https://support.sw.siemens.com/en-US/product/1009925838/
Nucleus ReadyStart V4: All versions < V4.1.1 only affected by CVE-2021-31344, CVE-2021-31346, CVE-2021-31885, CVE-2021-31890	Update to V4.1.1 or later version https://support.sw.siemens.com/en-US/product/1336134128/
Nucleus Source Code: All versions	Contact customer support to receive patch and update information

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 devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens’ operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Nucleus NET module incorporates a wide range of standard-compliant networking and communication protocols, drivers, and utilities to deliver full-featured network support in any embedded device. The networking functionality is fully integrated into the Nucleus RTOS and supports a variety of processors and MCUs.

Nucleus ReadyStart is a platform with integrated software IP, tools, and services ideal for applications where a small footprint, deterministic performance, and small code size are essential.

Nucleus RTOS is a highly scalable micro-kernel based real-time operating system designed for scalability and reliability in systems spanning the range of aerospace, industrial, and medical applications. Since V3, Nucleus RTOS (incl. its modules, e.g. Nucleus NET) is an integral part of the Nucleus ReadyStart platform.

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-2021-31881

When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008)

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-31882

The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011)

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/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-2021-31883

When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013)

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/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-2021-31884

The DHCP client application assumes that the data supplied with the “Hostname” DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

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-2021-31886

FTP server does not properly validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010)

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2021-31887

FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2021-31888

FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Yuval Halaban, Uriel Malin, and Tal Zohar from Medigate for coordinated disclosure
- Daniel dos Santos, Amine Amri, and Stanislav Dashevskyi from Forescout Technologies for coordinated disclosure

ADDITIONAL INFORMATION

For more details regarding the NUCLEUS:13 vulnerabilities in the Nucleus TCP/IP stack refer to the Forescout Publication “NUCLEUS:13” at https://www.forescout.com/research-labs/nucleus-13

Nucleus ReadyStart V3: Several vulnerabilities were already fixed in versions before V2017.02.4:

- V2012.08 and later already fix CVE-2021-31881
- V2013.08.1 and later already fix CVE-2021-31886
- V2014.12 and later already fix CVE-2021-31345
- V2017.02.1 and later already fix CVE-2021-31882, CVE-2021-31883, CVE-2021-31884, CVE-2021-31887, CVE-2021-31888

- V2017.02.3 and later already fix CVE-2021-31889

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 (2021-11-09): Publication Date
V1.1 (2021-12-14): Moved product CAPITAL VSTAR to a separate advisory (SSA-620288)

TERMS OF USE