SSA-620288: Multiple Vulnerabilities (NUCLEUS:13) in Capital Embedded AR Classic

Publication Date: 2021-12-14
Last Update: 2024-10-08
Current Version: V1.2
CVSS v3.1 Base Score: 8.2
CVSS v4.0 Base Score: 6.9

SUMMARY

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

Capital Embedded AR Classic uses an affected version of the Nucleus software and inherently contains several of these vulnerabilities.

Siemens has released a new version for Capital Embedded AR Classic R20-11 and recommends to update to the latest version. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Capital Embedded AR Classic 431-422: All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Capital Embedded AR Classic R20-11: All versions < V2303 affected by all CVEs	Update to V2303 or later version See further 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:

- CVE-2021-31344, CVE-2021-31345, CVE-2021-31346, CVE-2021-31889, CVE-2021-31890: Apply network segmentation and put the ECUs behind properly configured gateways/firewalls
- CVE-2021-31881, CVE-2021-31882, CVE-2021-31883: Disable DHCP client functionality, if feature not used, by deselecting the TcpIpIpV4General/TcpIpDhcpClientEnabled Pre-Compile configuration option

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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

Capital Embedded AR Classic (formerly called Capital VSTAR), is a scalable AUTOSAR Classic software platform that meets ISO 26262 use cases for up to ASIL D. Versions are available for several recent AUTOSAR Classic releases, including 4.3.1 and 20-11. Although not based on Nucleus RTOS, Embedded AR Classic includes its networking module, Nucleus NET.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

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
CVSS v4.0 Base Score	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
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
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
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
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
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
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

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
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
CWE	CWE-240: Improper Handling of Inconsistent Structural Elements

ADDITIONAL INFORMATION

Products listed in this advisory use Nucleus NET, the networking stack of 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/html/ssa-044112.html

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 (2021-12-14):	Publication Date
V1.1 (2022-11-08):	Removed CVE-2021-31884 as Capital VSTAR is not affected
V1.2 (2024-10-08):	Renamed Capital VSTAR to Capital Embedded AR Classic; added fix for version line R20-11

TERMS OF USE