SSA-434032: Input Validation Vulnerability in the DHCP Client of Nucleus RTOS

Publication Date:	2019-11-12
Last Update:	2024-02-13
Current Version:	V1.1
CVSS v3.1 Base Score:	7.1
CVSS v4.0 Base Score:	7.1

SUMMARY

The DHCP implementation of the networking component (Nucleus NET) in Nucleus Real-Time Operating System (RTOS) contains a vulnerability that could allow an attacker to change the IP address of an affected device to an invalid value.

Siemens has released new versions for several affected products and recommends to update to the latest versions. 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 Disable DHCP client functionality, if feature not used, by deselecting the TcpIpIpV4General/TcpIpDhcpClientEnabled Pre-Compile configuration option See further 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 Disable DHCP client functionality, if feature not used, by deselecting the TcpIpIpV4General/TcpIpDhcpClientEnabled Pre-Compile configuration option See further recommendations from section Workarounds and Mitigations
Nucleus NET: All versions affected by all CVEs	Currently no fix 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 See further recommendations from section Workarounds and Mitigations
Nucleus ReadyStart V3: All versions < V2017.02.3 affected by all CVEs	Update to V2017.02.3 or later version https://support.sw.siemens.com/en-US/product/1009925838/ See further recommendations from section Workarounds and Mitigations

Nucleus Source Code: All versions affected by all CVEs	Contact customer support to receive patch and update information 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:

- Avoid using DHCP Client of Nucleus NET

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

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 ("Nucleus PLUS") 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.

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-2019-13939

By sending specially crafted DHCP packets to a device where the DHCP client is enabled, an attacker could change the IP address of the device to an invalid value.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.1
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:H/SC:N/SI:N/SA:N
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Armis for reporting the vulnerability
- Cybersecurity and Infrastructure Security Agency (CISA) for coordinated disclosure

ADDITIONAL INFORMATION

Note: Nucleus SafetyCert is not affected since it leverages the LWNET stack which is not affected. The Nucleus SafetyCert bundle however, does include a copy of Nucleus ReadyStart to allow easier prototyping, which is affected as noted above.

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 (2019-11-12):	Publication Date
V1.1 (2024-02-13):	Consolidated list of products; renamed Capital VSTAR to Capital Embedded AR Classic; added fix and mitigation for Capital Embedded AR Classic; added CVSSv4.0 vector and score

TERMS OF USE