SSA-248289: Denial of Service Vulnerabilities in the IPv6 Stack of Nucleus RTOS

Publication Date: 2021-04-13
Last Update: 2024-02-13
Current Version: V1.2
CVSS v3.1 Base Score: 7.5
CVSS v4.0 Base Score: 8.7

SUMMARY

The IPv6 stack of the networking component (Nucleus NET) in Nucleus Real-Time Operating System (RTOS) contains two vulnerabilities when processing IPv6 headers which could allow an attacker to cause a denial of service condition.

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 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 IPv6 functionality, if feature not used, by deselecting the TcpIpIpV6General/IpV6Enabled Pre-Compile configuration option
Capital Embedded AR Classic R20-11: All versions < V2303 affected by all CVEs	Update to V2303 or later version Disable IPv6 functionality, if feature not used, by deselecting the TcpIpIpV6General/IpV6Enabled Pre-Compile configuration option
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
Nucleus ReadyStart V3: All versions < V2017.02.4 affected by all CVEs	Update to V2017.02.4 or later version https://support.sw.siemens.com/en-US/product/1009925838/
Nucleus ReadyStart V4: All versions < V4.1.0 affected by all CVEs	Update to V4.1.0 or later version https://support.sw.siemens.com/en-US/product/1336134128/
Nucleus Source Code: All versions including affected IPv6 stack affected by all CVEs	Contact customer support to receive patch and update information

WORKAROUNDS AND MITIGATIONS

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-2021-25663

The function that processes IPv6 headers does not check the lengths of extension header options, allowing attackers to put this function into an infinite loop with crafted length values.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability CVE-2021-25664

The function that processes the Hop-by-Hop extension header in IPv6 packets and its options lacks any checks against the length field of the header, allowing attackers to put the function into an infinite loop by supplying arbitrary length values.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

ADDITIONAL INFORMATION

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 (2021-04-13):	Publication Date
V1.1 (2021-11-09):	Added solution for Nucleus ReadyStart V3; consolidated list of products
V1.2 (2024-02-13):	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