SSA-705111: Multiple Vulnerabilities (NAME:WRECK) in the DNS Module of Nucleus RTOS

Publication Date: 2021-04-13
Last Update: 2022-01-11
Current Version: V1.2
CVSS v3.1 Base Score: 6.5

SUMMARY

Security researchers discovered and disclosed 9 vulnerabilities in several DNS implementations, also known as “NAME:WRECK” vulnerabilities. The vulnerabilities described in this advisory are from this set.

The DNS client of affected products contains multiple vulnerabilities related to the handling of DNS responses and requests. The most severe could allow an attacker to manipulate the DNS responses and cause a denial-of-service condition.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific 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 See further recommendations from section Workarounds and Mitigations
Nucleus ReadyStart V3: All versions < V2017.02.3	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 ReadyStart V3: All versions < V2017.02.4 only affected by CVE-2021-25677	Update to V2017.02.4 or later version https://support.sw.siemens.com/en-US/product/1009925838/ See further recommendations from section Workarounds and Mitigations
Nucleus ReadyStart V4: All versions < V4.1.0	Update to V4.1.0 or later version https://support.sw.siemens.com/en-US/product/1336134128/ See further recommendations from section Workarounds and Mitigations
Nucleus Source Code: Versions including affected DNS modules	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 DNS client of affected versions

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 VSTAR is an efficient implementation of the AUTOSAR standard. It is a complete solution including tools and a software platform to meet engineers' needs, from creating ECU extract updates to software platform configurations. Although not based on Nucleus RTOS, VSTAR includes its networking module, Nucleus NET.

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-2020-27736

The DNS domain name label parsing functionality does not properly validate the null-terminated name in DNS-responses. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the read memory.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2020-27737

The DNS response parsing functionality does not properly validate various length and counts of the records. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the memory past the allocated structure.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/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-2020-27738

The DNS domain name record decompression functionality does not properly validate the pointer offset values. The parsing of malformed responses could result in a read access past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-788: Access of Memory Location After End of Buffer

Vulnerability CVE-2021-25677

The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving.

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-330: Use of Insufficiently Random Values

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Daniel dos Santos from Forescout Technologies for coordinated disclosure

ADDITIONAL INFORMATION

['Some products that include the Nucleus products are also affected as in SSA-669158.']

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 CVE-2021-25677 in Nucleus ReadyStart V3; consolidated list of products
V1.2 (2022-01-11):	Removed CAPITAL VSTAR as not affected

TERMS OF USE