SSA-185699: Out of Bounds Write 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: 8.1

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 the networking component (Nucleus NET) in Nucleus Real-Time Operating System (RTOS) contains two out of bounds write vulnerabilities in the handling of DNS responses that could allow an attacker to cause a denial-of-service condition or to remotely execute code.

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 < V5.2	Currently no remediation is planned Update to the latest version of Nucleus ReadyStart V3 or V4 Note that the latest version of Nucleus NET (V5.2) is not affected, but is already beyond end of software support Contact customer support or your local Nucleus Sales team for mitigation advice 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 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-2020-15795

The DNS domain name label parsing functionality does not properly validate the names in DNS-responses. The parsing of malformed responses could result in a write past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to execute code in the context of the current process or cause a denial-of-service condition.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2020-27009

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

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-823: Use of Out-of-range Pointer Offset

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Daniel dos Santos from Forescout Technologies Inc. for coordinated disclosure

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): Consolidated list of products
V1.2 (2022-01-11): Removed CAPITAL VSTAR as not affected

TERMS OF USE