

SSA-185699: Out of Bounds Write Vulnerabilities (NAME:WRECK) in the DNS Module of Nucleus Products

Publication Date: 2021-04-13
Last Update: 2021-04-13
Current Version: V1.0
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 advisories are from this set.

The DNS client of affected products 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, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Nucleus NET: All versions < V5.2	See recommendations from Section Workarounds and Mitigations or upgrade to the latest versions of Nucleus ReadyStart or Nucleus 4 Note that the latest version of Nucleus NET (V5.2) is not affected by the vulnerabilities, but is already beyond end of software support
Nucleus RTOS: versions including affected DNS modules	Contact customer support to receive patch and update information
Nucleus Source Code: versions including affected DNS modules	Contact customer support to receive patch and update information
VSTAR: versions including affected DNS modules	Contact customer support to receive patch and update information

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
- For additional mitigation advice please contact customer support or your local Nucleus Sales team

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 and supports a variety of processors and MCUs.

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

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.