SSA-362164: Predictable Initial Sequence Numbers in the TCP/IP Stack of Nucleus RTOS

Publication Date: 2021-02-09
Last Update: 2022-11-08
Current Version: V1.2
CVSS v3.1 Base Score: 6.5

SUMMARY

The networking component (Nucleus NET) in Nucleus Real-Time Operating System (RTOS) use Initial Sequence Numbers for TCP-Sessions that are predictable.

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 fix 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 ReadyStart V3: All versions < V2012.12	Update to V2012.12 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	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:

- Protect transmitted data with cryptographic protocols such as Transport Layer Security

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 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-2020-28388

Initial Sequence Numbers (ISNs) for TCP connections are derived from an insufficiently random source. As a result, the ISN of current and future TCP connections could be predictable. An attacker could hijack existing sessions or spoof future ones.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-342: Predictable Exact Value from Previous Values

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Daniel dos Santos from Forescout Technologies 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 (2021-02-09): Publication Date
V1.1 (2021-11-09): Consolidated list of products
V1.2 (2022-11-08): Removed Capital VSTAR as it is not affected by CVE-2022-28388

TERMS OF USE