SSA-362164: Predictable Initial Sequence Numbers in Mentor Nucleus TCP stack

Publication Date: 2021-02-09
Last Update: 2021-02-09
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

Some versions of Mentor Nucleus ReadyStart and Nucleus NET use Initial Sequence Numbers for TCP-Sessions that are predictable.

Siemens has released updates for the affected products and recommends to update to the latest version(s).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Nucleus NET: All versions < V5.2	See recommendations from Section Workarounds and Mitigations or update to the latest version of Nucleus ReadyStart.
Nucleus ReadyStart for ARM, MIPS, and PPC: All versions < V2012.12	Update to V2012.12 or later version https://support.sw.siemens.com/en-US/product/1009925838/downloads

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

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.

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 parties for their 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

TERMS OF USE