SSA-434032: Vulnerability in Mentor Nucleus Networking Module

Publication Date: 2019-11-12
Last Update: 2019-11-12
Current Version: V1.0
CVSS v3.0 Base Score: 7.1

SUMMARY

Mentor Nucleus by Mentor, a Siemens Business, is affected by one vulnerability. This vulnerability could allow an attacker to affect the integrity and availability of the device.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Nucleus NET: All versions	See recommendations from section Workarounds and Mitigations or upgrade Nucleus ReadyStart and apply the corresponding patch.
Nucleus RTOS: All versions	See recommendations from section Workarounds and Mitigations or upgrade Nucleus ReadyStart and apply the corresponding patch.
Nucleus ReadyStart for ARM, MIPS, and PPC: All versions < V2017.02.2 with patch “Nucleus 2017.02.02 Nucleus NET Patch”	Upgrade to V2017.02.2 and install the patch “Nucleus 2017.02.02 Nucleus NET Patch” Updated firmware versions can be obtained from Mentor supportcenter: https://support.mentor.com/en/product/1009925838/downloads
Nucleus SafetyCert: All versions	Nucleus SafetyCert is non affected since it leverages the LWNET stack which is not affected. The Nucleus SafetyCert bundle however, does include a copy of Nucleus ReadyStart to allow easier prototyping, which is affected as noted above.
Nucleus Source Code: All versions	See recommendations from section Workarounds and Mitigations
VSTAR: All versions	Contact customer support to receive patch and update instructions.

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Avoid using DHCP Client of Nucleus NET

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

The Nucleus RTOS provides 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.

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.

VSTAR is a complete AUTOSAR 4 based ECU solution providing the tools and embedded software for on-time product deployment. The VSTAR implementation enables scalable support from resource limited small ECUs to powerful multi core solutions. The VSTAR modules developed according to ISO 26262 requirements can be used to address up to and including ASIL D use-cases.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2019-13939

By sending specially crafted DHCP packets to a device, an attacker may be able to affect availability and integrity of the device. Adjacent network access, but no authentication and no user interaction is needed to conduct this attack.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.1
CVSS Vector	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Armis for reporting the vulnerability.
- The Cybersecurity and Infrastructure Security Agency (CISA) 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 (2019-11-12): Publication Date

TERMS OF USE