SSA-313313: Denial of Service Vulnerability in the FTP Server of Nucleus RTOS

Publication Date: 2022-10-11
Last Update: 2023-02-14
Current Version: V1.2
CVSS v3.1 Base Score: 7.5

SUMMARY

The FTP server of the networking component (Nucleus NET) in Nucleus Real-Time Operating System (RTOS) does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Nucleus NET for Nucleus PLUS V1: All versions < V5.2a	Update to V5.2a as available in Nucleus PLUS V1.15 and apply the patch “v2022.11” https://support.sw.siemens.com/en-US/product/852852095/ See further recommendations from section Workarounds and Mitigations
Nucleus NET for Nucleus PLUS V2: All versions < V5.4	Update to V5.4 as available in Nucleus PLUS V2.1f and apply the patch “v2022.11” https://support.sw.siemens.com/en-US/product/852852095/ See further recommendations from section Workarounds and Mitigations
Nucleus ReadyStart V3 V2012: All versions < V2012.08.1	Update to V2012.08.1 and apply the patch “v2022.11” https://support.sw.siemens.com/en-US/product/1009925838/ See further recommendations from section Workarounds and Mitigations
Nucleus ReadyStart V3 V2017: All versions < V2017.02.4	Update to V2017.02.4 and apply the patch “2017.02.4_patch_CVE-2022-38371” https://support.sw.siemens.com/en-US/product/1009925838/ See further recommendations from section Workarounds and Mitigations
Nucleus Source Code: Versions including affected FTP server	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:

- Configure `TCP_MAX_KEEPALIVES` to a lower value such as 3. Additionally, configure `TCP_KEEPALIVE_INTERVAL` and `TCP_KEEPALIVE_DELAY` be set to 3 seconds. Rebuild your application.

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 ("Nucleus PLUS") 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-2022-38371

The FTP server does not properly release memory resources that were reserved for incomplete connection attempts by FTP clients. This could allow a remote attacker to generate a denial of service condition on devices that incorporate a vulnerable version of the FTP server.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Kaspersky Lab ICS CERT for coordinated disclosure
- WAGO for reporting the vulnerability and coordination efforts

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 (2022-10-11):	Publication Date
V1.1 (2022-12-13):	Added specific mitigation
V1.2 (2023-02-14):	Added fix for Nucleus NET in Nucleus PLUS V1, V2, and for Nucleus ReadyStart V2012

TERMS OF USE