SSA-935500: Denial of Service Vulnerability in FTP Server of Nucleus RTOS based APOGEE, TALON and Desigo PXC/PXM Products

Publication Date: 2022-10-11
Last Update: 2022-10-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

A denial of service vulnerability has been identified in the Nucleus RTOS (real-time operating system) and reported in the Siemens Security Advisory SSA-313313: https://cert-portal.siemens.com/productcert/html/ssa-313313.html.

The products listed below use affected versions of the Nucleus software and inherently contain the vulnerability.

Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
APOGEE MBC (PPC) (BACnet): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
APOGEE MBC (PPC) (P2 Ethernet): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
APOGEE MEC (PPC) (BACnet): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
APOGEE MEC (PPC) (P2 Ethernet): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
APOGEE PXC Compact (BACnet): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
APOGEE PXC Compact (P2 Ethernet): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
APOGEE PXC Modular (BACnet): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
APOGEE PXC Modular (P2 Ethernet): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC00-E.D: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations

Desigo PXC00-U: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC001-E.D: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC12-E.D: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC22-E.D: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC22.1-E.D: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC36.1-E.D: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC50-E.D: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC64-U: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC100-E.D: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC128-U: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC200-E.D: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXM20-E: All versions >= V2.3	Currently no fix is available See recommendations from section Workarounds and Mitigations
TALON TC Compact (BACnet): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
TALON TC Modular (BACnet): All versions	Currently no fix is available See 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:

- Disable the FTP service (Note that the FTP service is disabled by default on APOGEE, Desigo, and TALON products.)

Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

The APOGEE MEC and the MBC are high-performance Direct Digital Control (DDC) devices and are an integral part of the APOGEE Automation System.

The APOGEE PXC Modular and Compact Series are high-performance Direct Digital Control (DDC) devices and an integral part of the APOGEE Automation System.

The Desigo PX automation stations and operator units control and monitor building automation systems. They allow for alarm signaling, time-based programs and trend logging.

The TALON TC Modular and Compact Series are high-performance Direct Digital Control (DDC) devices and an integral part of the TALON Automation System.

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

ADDITIONAL INFORMATION

Products listed in this advisory use the Nucleus RTOS (Real-time operating system).

For more details regarding the vulnerability reported for Nucleus RTOS refer to Siemens Security Advisory SSA-313313: https://cert-portal.siemens.com/productcert/pdf/ssa-313313.pdf

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

TERMS OF USE