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: 2024-05-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.5
CVSS v4.0 Base Score: 8.7

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
APOGEE MBC (PPC) (BACnet): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
APOGEE MBC (PPC) (P2 Ethernet): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
APOGEE MEC (PPC) (BACnet): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
APOGEE MEC (PPC) (P2 Ethernet): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
APOGEE PXC Compact (BACnet): All versions < V3.5.7 affected by all CVEs	Update to V3.5.7 or later version https://partnerportal.extranet.dc.siemens.com/ See further recommendations from section Workarounds and Mitigations
APOGEE PXC Compact (P2 Ethernet): All versions < V2.8.21 affected by all CVEs	Update to V2.8.21 or later version https://partnerportal.extranet.dc.siemens.com/ See further recommendations from section Workarounds and Mitigations

APOGEE PXC Modular (BACnet): All versions < V3.5.7 affected by all CVEs	Update to V3.5.7 or later version https://partnerportal.extranet.dc.siemens.com/ See further recommendations from section Workarounds and Mitigations
APOGEE PXC Modular (P2 Ethernet): All versions < V2.8.21 affected by all CVEs	Update to V2.8.21 or later version https://partnerportal.extranet.dc.siemens.com/ See further recommendations from section Workarounds and Mitigations
Desigo PXC00-E.D: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC00-U: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC001-E.D: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC12-E.D: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC22-E.D: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC22.1-E.D: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC36.1-E.D: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC50-E.D: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC64-U: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC100-E.D: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations

Desigo PXC128-U: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXC200-E.D: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Desigo PXM20-E: All versions >= V2.3 affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
TALON TC Compact (BACnet): All versions < V3.5.7 affected by all CVEs	Update to V3.5.7 or later version https://partnerportal.extranet.dc.siemens.com/ See further recommendations from section Workarounds and Mitigations
TALON TC Modular (BACnet): All versions < V3.5.7 affected by all CVEs	Update to V3.5.7 or later version https://partnerportal.extranet.dc.siemens.com/ 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:

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

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 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

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

Desigo PXC00/64/128-U are automation stations with P-bus and PPS2 connections.

Desigo PXC00-E.D: System controller BACnet/IP. Article No: BPZ:PXC00-E.D

Desigo PXC001-E.D: System controller for the integration of KNX, M-Bus, Modbus or SCL over BACnet/IP. Article No: S55372-C114

Desigo PXC100-E.D: Automation station BACnet/IP, with up to 200 data points. Article No: BPZ:PXC100-E.D

Desigo PXC12-E.D: Automation station with 12 data points and BACnet on IP. Article No: BPZ:PXC12-E.D

Desigo PXC200-E.D: Automation station BACnet/IP, with more than 200 data points. Article No: BPZ:PXC200-E.D

Desigo PXC22-E.D: Automation station with 22 data points and BACnet on IP. Article No: BPZ:PXC22-E.D

Desigo PXC22.1-E.D: Automation station with 22 data points, extendable and BACnet on IP. Article No: S55372-C119

Desigo PXC36.1-E.D: Automation station with 36 data points, extendable and BACnet on IP. Article No: S55372-C121

Desigo PXC50-E.D: Automation station BACnet/IP, with up to 80 data points. Article No: S55372-C110

Desigo PXM20-E: Operator unit with BACnet on IP. Article No: BPZ:PXM20-E

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

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
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
V1.1 (2024-05-14):	Added fix for APOGEE PXC Series (BACnet), APOGEE PXC Series (P2 Ethernet), TALON TC Series (BACnet); added CVSSv4.0 vector and score

TERMS OF USE