SSA-114589: Multiple Vulnerabilities in Nucleus RTOS based APOGEE, TALON and Desigo PXC/PXM Products

Publication Date: 2021-11-09
Last Update: 2021-12-14
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

Multiple vulnerabilities (also known as “NUCLEUS:13”) have be identified in the Nucleus RTOS (real-time operating system) and reported in the Siemens Security Advisory SSA-044112: https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf.

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

Siemens is preparing updates and 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 remediation is planned See recommendations from section Workarounds and Mitigations
APOGEE MBC (PPC) (P2 Ethernet): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
APOGEE MEC (PPC) (BACnet): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
APOGEE MEC (PPC) (P2 Ethernet): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
APOGEE PXC Compact (BACnet): All versions	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
APOGEE PXC Compact (P2 Ethernet): All versions	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
APOGEE PXC Modular (BACnet): All versions	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
APOGEE PXC Modular (P2 Ethernet): All versions	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations

Desigo PXC00-E.D: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC00-U: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC001-E.D: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC12-E.D: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC22-E.D: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC22.1-E.D: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC36.1-E.D: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC50-E.D: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC64-U: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC100-E.D: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC128-U: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
Desigo PXC200-E.D: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations

Desigo PXM20-E: All versions >= V2.3	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
TALON TC Compact (BACnet): All versions	Remediation is planned (see section Additional Information) See further recommendations from section Workarounds and Mitigations
TALON TC Modular (BACnet): All versions	Remediation is planned (see section Additional 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:

- CVE-2021-31881, CVE-2021-31882, CVE-2021-31883, CVE-2021-31884: Disable the DHCP client and use static IP address configuration instead (Note that the DHCP client is disabled by default on APOGEE/TALON and Desigo products.)
- CVE-2021-31885, CVE-2021-31886, CVE-2021-31887, CVE-2021-31888: Disable the FTP service (Note that the FTP service is disabled by default on Desigo products.)
- Apply general security measures, especially:
  - Restrict system access to authorized personnel and follow a least privilege approach
  - Protect network access to the affected devices with appropriate measures, e.g. firewalls, to reduce the risk
  - Apply appropriate strategies for mitigation on the network level to ensure affected devices are as segmented
  - Ensure that default passwords are changed
  - Implement defense in depth concepts to mitigate risk of an attacker gaining access to affected devices and networks

  Please contact your local Siemens office for support.

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-2021-31344

ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network. (FSMD-2021-0004)

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

Vulnerability CVE-2021-31345

The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on a user-defined applications that runs on top of the UDP protocol. (FSMD-2021-0006)

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-1284: Improper Validation of Specified Quantity in Input

Vulnerability CVE-2021-31346

The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0007)

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-1284: Improper Validation of Specified Quantity in Input

Vulnerability CVE-2021-31881

When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0008)

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-31882

The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions. (FSMD-2021-0011)

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-31883

When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions. (FSMD-2021-0013)

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-31884

The DHCP client application assumes that the data supplied with the “Hostname” DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions. (FSMD-2021-0014)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2021-31885

TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands. (FSMD-2021-0009)

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-805: Buffer Access with Incorrect Length Value

Vulnerability CVE-2021-31886

FTP server does not properly validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0010)

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2021-31887

FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0016)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2021-31888

FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in Denial-of-Service conditions and Remote Code Execution. (FSMD-2021-0018)

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2021-31889

Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions. (FSMD-2021-0015)

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-191: Integer Underflow (Wrap or Wraparound)

Vulnerability CVE-2021-31890

The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory. (FSMD-2021-0017)

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-240: Improper Handling of Inconsistent Structural Elements

ADDITIONAL INFORMATION

Siemens is working to develop a solution to resolve the issues identified with the emphasis on addressing vulnerabilities that do not have a specific mitigation first.

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

For more details regarding the vulnerabilities reported for Nucleus RTOS refer to Siemens Security Advisory SSA-044112: https://cert-portal.siemens.com/productcert/pdf/ssa-044112.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 (2021-11-09): Publication Date
V1.1 (2021-12-14): Added affected Desigo PXC/PXM products; updated corresponding mitigation measures; informed about planned solutions

TERMS OF USE