SSA-162506: DHCP Client Vulnerability in SIMOTICS CONNECT 400, Desigo PXC/PXM, APOGEE MEC/MBC/PXC, APOGEE PXC Series, and TALON TC Series

Publication Date: 2020-04-14
Last Update: 2020-04-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.1

SUMMARY

SIMOTICS CONNECT 400, Desigo (Power PC-based), APOGEE MEC/MBC/PXC and TALON TC products are affected by a DHCP Client vulnerability as initially reported in SSA-434032 for the Mentor Nucleus Networking Module.

Siemens has released updates for some products and is working on further updates. For the remaining affected products, Siemens recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
APOGEE MEC/MBC/PXC (P2): All versions < V2.8.2	Use static IP address configuration
APOGEE PXC Series (BACnet): All versions >= V3.0	See recommendations from section Workarounds and Mitigations
APOGEE PXC Series (P2): All versions >= V2.8.2	See recommendations from section Workarounds and Mitigations
Desigo PXC (Power PC): All versions >= V2.3x	See recommendations from section Workarounds and Mitigations
Desigo PXM20 (Power PC): All versions >= V2.3x	See recommendations from section Workarounds and Mitigations
SIMOTICS CONNECT 400: All versions <= V0.3.0.95	Update to V0.3.0.330 https://support.industry.siemens.com/cs/ww/en/view/109778383
TALON TC Series (BACnet): All versions >= V3.0	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 DHCP client and use static IP address configuration instead (Note that the DHCP client is disabled by default on APOGEE/TALON and Desigo products.)
- APOGEE MEC, MBC, PXC (versions prior to V2.8.2): Use static IP address configuration as

described above

- APOGEE PXC Series, TALON TC Series, and Desigo products: If using static IP address is not possible, please contact your local Siemens office for support

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

SIMOTICS CONNECT 400 is a connector and sensor box, mounted on low-voltage motors to provide analytics data for the MindSphere application SIDRIVE IQ Fleet.

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

The APOGEE MEC (Modular Equipement Controller), MBC (Modular Building Controller), and PXC are Direct Digital Control (DDC) devices and an integral part of the APOGEE Automation System. These are legacy devices, replaced by the APOGEE PXC Modular and Compact Series.

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-2019-13939

By sending specially crafted DHCP packets to a device where the DHCP client is enabled, an attacker could change the IP address of the device to an invalid value.

The vulnerability could affect availability and integrity of the device. Adjacent network access is required, but no authentication and no user interaction is needed to conduct an attack.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-840: Business Logic Errors

ADDITIONAL INFORMATION

Products listed in this advisory are based on Mentor Nucleus NET. See SSA-434032 for the related security advisory.

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 (2020-04-14): Publication Date

TERMS OF USE