SSA-662649: Denial of Service Vulnerability in Desigo DXR and PXC Controllers

Publication Date: 2022-05-10
Last Update: 2022-05-10
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability in Desigo DXR and PXC controllers has been identified that could allow an attacker to disable and reset a device to factory state using a denial of service attack.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Desigo DXR2: All versions < V01.21.142.5-22	Update to V01.21.142.5-22 or later version
Desigo PXC3: All versions < V01.21.142.4-18	Update to V01.21.142.4-18 or later version
Desigo PXC4: All versions < V02.20.142.10-10884	Update to V02.20.142.10-10884 or later version
Desigo PXC5: All versions < V02.20.142.10-10884	Update to V02.20.142.10-10884 or later version

WORKAROUNDS AND MITIGATIONS

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

The Desigo DXR2 controllers are compact, programmable automation stations with increased functionality and flexibility to support the demands for standard control of terminal HVAC equipment and TRA (Total Room Automation) applications.

The Desigo PXC3 series room automation stations can be used for buildings with more sophisticated requirements on functionality and flexibility. Desigo Room Automation is used when several disciplines (HVAC, lighting, shading) are combined to form one solution and when high flexibility is required.

The Desigo PXC4 building automation controller was designed for HVAC systems controls. It was developed as a compact device with built in IOs with the ability to expand to your needs using addition TX-IO modules.

The Desigo PXC5 is a freely programmable controller for BACnet system-level functions such as alarm routing, system-wide scheduling and trending, as well as device monitoring.

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-2021-41545

When the controller receives a specific BACnet protocol packet, an exception causes the BACnet communication function to go into a "out of work" state and could result in the controller going into a "factory reset" state.

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-248: Uncaught Exception

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 (2022-05-10): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/

terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.