SSA-824231: Unauthenticated Firmware Upload Vulnerability in Desigo PX Controllers

Publication Date: 2018-01-24
Last Update: 2019-03-12
Current Version: V1.3
CVSS v3.0 Base Score: 9.8

SUMMARY

The latest update for Desigo PXC devices fixes a vulnerability that could allow unauthenticated remote attackers to upload malicious firmware without prior authentication.

Siemens recommends updating to the new version.

AFFECTED PRODUCTS AND SOLUTION

This advisory covers only the Desigo PX Controller product line and not the Apogee PX Controller product line.

Affected Product and Versions	Remediation
Desigo Automation Controllers Compact PXC12/22/36-E.D: All versions < V6.00.204	Install V6.00.204 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers Compact PXC12/22/36-E.D: All versions < V5.10.069	Install V5.10.069 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers Compact PXC12/22/36-E.D: All versions < V5.00.171	Install V5.00.171 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers Compact PXC12/22/36-E.D: All versions < V4.10.111	Install V4.10.111 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers Modular PXC00/50/100/200-E.D: All versions < V6.00.204	Install V6.00.204 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers Modular PXC00/50/100/200-E.D: All versions < V5.10.069	Install V5.10.069 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers Modular PXC00/50/100/200-E.D: All versions < V5.00.171	Install V5.00.171 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers Modular PXC00/50/100/200-E.D: All versions < V4.10.111	Install V4.10.111 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.

Desigo Automation Controllers PXC00/64/128-U with Web module: All versions < V6.00.204	Install V6.00.204 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers PXC00/64/128-U with Web module: All versions < V5.10.069	Install V5.10.069 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers PXC00/64/128-U with Web module: All versions < V5.00.171	Install V5.00.171 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers PXC00/64/128-U with Web module: All versions < V4.10.111	Install V4.10.111 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers for Integration PXC001-E.D: All versions < V6.00.204	Install V6.00.204 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers for Integration PXC001-E.D: All versions < V5.10.069	Install V5.10.069 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers for Integration PXC001-E.D: All versions < V5.00.171	Install V5.00.171 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Automation Controllers for Integration PXC001-E.D: All versions < V4.10.111	Install V4.10.111 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Operator Unit PXM20-E: All versions < V6.00.204	Install V6.00.204 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Operator Unit PXM20-E: All versions < V5.10.069	Install V5.10.069 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Operator Unit PXM20-E: All versions < V5.00.171	Install V5.00.171 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.
Desigo Operator Unit PXM20-E: All versions < V4.10.111	Install V4.10.111 or a later version Updated firmware versions can be obtained from Siemens customer support or a local partner.

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

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

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability (CVE-2018-4834)

A remote attacker with network access to the device could potentially upload a new firmware image to the devices without prior authentication.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Can Demirel and Melih Berk Ekşioğlu from Biznet Bilişim for coordinated disclosure
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts

ADDITIONAL INFORMATION

For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2018-01-24):	Publication Date
V1.1 (2018-02-05):	Removed broken links
V1.2 (2018-03-20):	Clarified that Apogee PX product line is out of scope
V1.3 (2019-03-12):	Older firmware versions added

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.