SSA-898181: Desigo PX Web Remote Denial of Service Vulnerability

Publication Date: 2019-11-12
Last Update: 2019-11-12
Current Version: V1.0
CVSS v3.1 Base Score: 5.3

SUMMARY

The latest update for Desigo PXC devices fixes a vulnerability that could allow unauthenticated remote users to cause a denial of service condition on the PX Web interface (HTTP, port tcp/80) of a device. Devices where PX Web is not enabled are not affected by this vulnerability.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Desigo PX automation controllers PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D with Desigo PX Web modules PXA40-W0, PXA40-W1, PXA40-W2: All firmware versions < V6.00.320	Install V6.00.320 or a later version https://support.industry.siemens.com/cs/document/109772802
Desigo PX automation controllers PXC00-U, PXC64-U, PXC128-U with Desigo PX Web modules PXA30-W0, PXA30-W1, PXA30-W2: All firmware versions < V6.00.320	Install V6.00.320 or a later version https://support.industry.siemens.com/cs/document/109772802
Desigo PX automation controllers PXC22.1-E.D, PXC36-E.D, PXC36.1-E.D with activated web server: All firmware versions < V6.00.320	Install V6.00.320 or a later version https://support.industry.siemens.com/cs/document/109772802

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Ensure that the PX Web interface is only accessible from trusted networks.

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 3.1 (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-2019-13927

The device contains a vulnerability that could allow an attacker to cause a denial of service condition on the device's web server by sending a specially crafted HTTP message to the web server port (tcp/80).

The security vulnerability could be exploited by an attacker with network access to an affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device's web service. While the device itself stays operational, the web server responds with HTTP status code 404 (Not found) to any further request. A reboot is required to recover the web interface.

At the time of advisory publication no public exploitation of this security vulnerability was known.

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:N/A:L/E:H/RL:O/RC:C
CWE	CWE-472: External Control of Assumed-Immutable Web Parameter

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Gjoko 'LiquidWorm' Krstic from Zero Science Lab (MK) for coordinated disclosure.

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 (2019-11-12): Publication Date

TERMS OF USE

additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.