

SSA-856492: Limited Entropy in PRNG of Desigo PX Web Modules

Publication Date 2016-12-16
Last Update 2016-12-16
Current Version V1.0
CVSS v3.0 Base Score 5.9

SUMMARY

The latest update for Desigo PX Web modules fixes a vulnerability that could allow remote attackers to recover private keys used for HTTPS in the integrated web server under certain conditions.

AFFECTED PRODUCTS

- Desigo PX Web modules PXA40-W0, PXA40-W1, PXA40-W2 for Desigo PX automation controllers PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D: All firmware versions < V6.00.046
- Desigo PX Web modules PXA30-W0, PXA30-W1, PXA30-W2 for Desigo PX automation controllers PXC00-U, PXC64-U, PXC128-U: All firmware versions < V6.00.046

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.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (<http://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 assessed by the customer to accomplish final scoring.

Vulnerability Description (CVE-2016-9154)

The affected devices use a pseudo random number generator with insufficient entropy to generate certificates for HTTPS, potentially allowing remote attackers to reconstruct the corresponding private key.

CVSS Base Score 5.9

CVSS Vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

Mitigating Factors

Applying a Defense-in-Depth concept and protecting the web interface at port 443/TCP from unauthorized access reduces the imposed risk. Siemens recommends operating these devices only within trusted networks.

SOLUTION

Siemens provides firmware update V6.00.046 [1] for the affected devices which fixes the vulnerability. The update is recommended to all customers operating an affected device.

Until patches can be applied, Siemens recommends the following:

- Protect network access
- Apply a Defense-in-Depth concept

- Restrict access to port 443/TCP of Desigo PX-Web modules
- Disable the web server

ACKNOWLEDGEMENTS

Siemens thanks Marcella Hastings, Joshua Fried and Nadia Heninger from the University of Pennsylvania for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] The firmware updates for Desigo PX Web modules can be obtained from:
<https://support.industry.siemens.com/cs/ww/en/view/109742824>

[2] 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 (2016-12-16): Publication Date

DISCLAIMER

See: https://www.siemens.com/terms_of_use