SSA-971654: Authentication Bypass in 7KT PAC1200 Data Manager from the SENTRON Portfolio

Publication Date 2017-10-05
Last Update 2017-10-05
Current Version V1.0
CVSS v3.0 Base Score 9.8

SUMMARY

The latest update for 7KT PAC1200 data manager (7KT1260) from the SENTRON portfolio fixes a vulnerability that could allow remote attackers to bypass the authentication mechanism and perform administrative actions under certain conditions.

AFFECTED PRODUCTS

- 7KT PAC1200 data manager (7KT1260) from the SENTRON portfolio: All versions < V2.03

DESCRIPTION

7KT PAC1200 data manager (7KT1260) from the SENTRON portfolio is a fully integrated smart meter with web interface.

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 (CVE-2017-9944)

The integrated web server (port 80/tcp) of the affected devices could allow unauthenticated remote attacker to perform administrative operations over the network.

CVSS 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

Mitigating Factors

The attacker must have network access to the affected devices. Siemens recommends operating the devices only within trusted networks [3].

SOLUTION

Siemens provides firmware version V2.03 [1] for 7KT PAC1200 data manager (7KT1260) from the SENTRON portfolio which fixes the vulnerability and recommends customers to update to the new fixed version.

As a general security measure Siemens strongly recommends to protect network access to the web server with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks Maxim Rupp for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] The firmware update V2.0.3 for 7KT PAC1200 data manager (7KT1260) from the SENTRON portfolio can be obtained at:
https://support.industry.siemens.com/cs/ww/de/view/109749883/en?dl=en

[2] Contact the Siemens Industry Technical Support Center at:
https://www.siemens.de/lowvoltage/support-request

[3] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[4] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[5] 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 (2017-10-05): Publication Date

DISCLAIMER