SSA-771218: Vulnerability in 7KM PAC Switched Ethernet PROFINET expansion module from the SENTRON portfolio

Publication Date 2017-08-30
Last Update 2017-08-30
Current Version V1.0
CVSS v3.0 Base Score 4.3

SUMMARY

The latest firmware version for 7KM PAC Switched Ethernet PROFINET expansion modules resolves a denial-of-service vulnerability.

AFFECTED PRODUCTS

- 7KM PAC Switched Ethernet PROFINET expansion module: All versions < V2.1.3

DESCRIPTION

The 7KM PAC Switched Ethernet PROFINET expansion module enables Ethernet PROFINET network access to the main devices 7KM PAC measuring devices and COM100/800 breaker data server for molded case circuit breaker (MCCB) devices.

The 7KM PAC measuring devices are used in electrical installations and power distribution to assess system state and power quality.

The COM100/800 breaker data server is used as a gateway and enables communication between the MCCB and automation systems.

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-2017-9945)

A Denial-of-Service condition could be induced by a specially crafted PROFINET DCP packet sent as a local Ethernet (Layer 2) broadcast. The affected component requires a manual restart via the main device to recover.

CVSS Base Score 4.3
CVSS Vector CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

Mitigating Factors

The attacker must have network access to the local Ethernet segment (Layer 2). Siemens recommends operating the devices only within trusted networks [3].

SOLUTION

Siemens provides firmware version V2.1.3 [1] for 7KM PAC Switched Ethernet PROFINET expansion modules 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 with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] The firmware update V2.1.3 for the 7KM PAC Switched Ethernet PROFINET expansion modules can be obtained at:
https://support.industry.siemens.com/cs/ww/en/view/109749555

[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 (2017-08-30): Publication Date

DISCLAIMER