SSA-296574: Denial of Service in SICAM RTU Devices

Publication Date 2016-10-21
Last Update 2016-10-21
Current Version V1.0
CVSS v3.0 Base Score 7.5

SUMMARY

The latest ETA4 firmware for the SM-2558 IEC 60870-5-104 COM Module fixes a vulnerability that could allow remote attackers to perform a Denial-of-Service attack under certain conditions.

For SM-2556 IEC 60870-5-104 COM Modules, customers are advised to contact the Siemens Energy Customer Support Center [3].

AFFECTED PRODUCTS

- ETA4 firmware (all versions < revision 08) of the SM-2558 extension module for
  - SICAM AK
  - SICAM TM 1703
  - SICAM BC 1703
  - SICAM AK 3
- ETA2 firmware (revision 11.01 and earlier) of the SM-2556 extension module for
  - SICAM AK
  - SICAM TM
  - SICAM BC

DESCRIPTION

The SM-2558 and SM-2556 communication modules are protocol elements for LAN/WAN communication with fast Ethernet 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 Description: (CVE-2016-7987)

Specially crafted packets sent to port 2404/TCP could cause the affected device to go into defect mode. A cold start might be required to recover the system under certain conditions.

CVSS Base Score 7.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

Mitigating Factors

The vulnerability can be mitigated by protecting network access to the affected devices. Siemens recommends operating the devices only within trusted networks [4].

SOLUTION

Siemens provides firmware ETA4 revision 08 [1] for SM-2558 which fixes the vulnerability and recommends customers update to the fixed version.

For the SM-2556 extension module, Siemens recommends customers contact the support center [3].

Until patches can be applied, Siemens advises to apply the following steps to mitigate the risk:

- Use a firewall or the IPsec functionality of the SM-2558 module [2] to restrict access to port 2404/TCP
- Always run RTUs in trusted networks

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms [4] (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- Stephan Beirer, Markus Mahrla, Toralf Gimpel, and Sebastian Krause, from GAI NetConsult GmbH, and Adam Crain, Automatak LLC for coordinated disclosure of the vulnerability.
- Bundesamt für Sicherheit in der Informationstechnik (BSI) for reporting the vulnerability and coordination efforts.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for reporting the vulnerability and coordination efforts.

ADDITIONAL RESOURCES

[1] The firmware update ETA4 revision 08 for SM-2558:
http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/substation-automation/substation-automation/Pages/Overview.aspx

[2] The SICAM RTUs ADMINISTRATOR Security Manual:
http://www.downloads.siemens.com/download-center/d/SIC_RTUs_ADMIN_SECURITY_ENG.pdf?mandator=ic_sg&segment=Global&fct=downloadasset&pos=download&id1=DLA05_43299

[3] Contact the Siemens Energy Customer Support Center at:
support.energy@siemens.com

[4] Recommended security guidelines to Secure Substation:
http://www.siemens.com/gridsecurity

[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 (2016-10-21): Publication Date

DISCLAIMER