SSA-323211: Vulnerabilities in SIPROTEC 4 and SIPROTEC Compact Devices

Publication Date 2017-07-04
Last Update 2017-12-22
Current Version V1.6
CVSS v3.0 Base Score 8.6

SUMMARY

SIPROTEC 4 and SIPROTEC Compact devices are affected by several vulnerabilities. Two of the vulnerabilities could allow attackers to perform a denial-of-service attack under certain conditions.

Siemens has released updates for several affected products, is working on updates for the remaining affected products, and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS

- Firmware variants for EN100 Ethernet modules as optional for SIPROTEC 4 and SIPROTEC Compact:
  - Firmware variant PROFINET IO: All versions < V1.04.01
  - Firmware variant Modbus TCP: All versions < V1.11.00
  - Firmware variant DNP3 TCP: All versions < V1.03
  - Firmware variant IEC 104: All versions < V1.21
- EN100 Ethernet module included in SIPROTEC Merging Unit 6MU80: All firmware versions < V1.02.02
- SIPROTEC 7SJ686 affected by vulnerability 2: All versions < V4.83
- SIPROTEC 7SJ686 affected by vulnerability 6: All versions < V4.87
- SIPROTEC 7UT686 affected by vulnerability 2: All versions < V4.01
- SIPROTEC 7UT686 affected by vulnerability 6: All versions < V4.02
- SIPROTEC 7SD686 affected by vulnerability 2: All versions < V4.03
- SIPROTEC 7SD686 affected by vulnerability 6: All versions < V4.05
- SIPROTEC 7SJ66 affected by vulnerability 2: All versions < V4.20
- SIPROTEC 7SJ66 affected by vulnerability 6: All versions

DESCRIPTION

SIPROTEC 4 and SIPROTEC Compact devices provide a wide range of integrated protection, control, measurement, and automation functions for electrical substations and other fields of application. The EN100 Ethernet modules are used for enabling IEC 61850 communication and either PROFINET IO, Modbus TCP, DNP3 TCP, IEC 104 or IEC 61850-9-2 communication with electrical/optical 100 Mbit interfaces for SIPROTEC 4 and SIPROTEC Compact devices.

SIPROTEC Merging Unit 6MU80 devices allows conversion of current substations to process bus substations based on IEC 61850-9-2 and IEC 61850-8-1 GOOSE without changing the primary equipment.

Detailed information about the vulnerabilities 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 1 (CVE-2015-5374)

Specially crafted packets sent to port 50000/UDP could cause a denial-of-service of the affected device. A manual reboot may be required to recover the service of the device.

CVSS Base Score 8.6
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:H/RL:O/RC:C

Vulnerability 2 (CVE-2016-4784)

The integrated web server (port 80/TCP) of the affected devices could allow remote attackers to obtain sensitive device information if network access was obtained.

CVSS Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability 3 (CVE-2016-4785)

The integrated web server (port 80/TCP) of the affected devices could allow remote attackers to obtain a limited amount of device memory content if network access was obtained.

CVSS Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability 4 (CVE-2016-7112)

Attackers with network access to the device's web interface (port 80/TCP) could possibly circumvent authentication and perform certain administrative operations.

CVSS Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability 5 (CVE-2016-7113)

Specially crafted packets sent to port 80/TCP could cause the affected device to go into defect mode.

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

Vulnerability 6 (CVE-2016-7114)

Attackers with network access to the device's web interface (port 80/TCP) could possibly circumvent authentication and perform certain administrative operations. A legitimate user must be logged into the web interface for the attack to be successful.

CVSS Base Score 4.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/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 updates that fix the vulnerabilities for the following affected products and recommends customers update to the new fixed version:

- Firmware variants for EN100 Ethernet modules as optional for SIPROTEC 4 and SIPROTEC Compact:

  - Firmware variant PROFINET IO: Update to V1.04.01 [1]
  - Firmware variant Modbus TCP: Update to V1.11.00 [1]
  - Firmware variant DNP3 TCP: Update to V1.03 [1]
  - Firmware variant IEC 104: Update to V1.21 [1]

- EN100 Ethernet module included in SIPROTEC Merging Unit 6MU80: Update to firmware V1.02.02 by contacting the Siemens energy hotline [2]
- SIPROTEC 7SJ66: update to firmware V4.20 [3] or higher to fix vulnerability 2
- SIPROTEC 7SJ686: update to firmware V4.86 [4] or higher to fix vulnerability 2
- SIPROTEC 7SJ686: update to firmware V4.87 [4] to fix vulnerability 6
- SIPROTEC 7UT686: update to firmware V4.01 [4] or higher to fix vulnerability 2
- SIPROTEC 7UT686: update to firmware V4.02 [4] to fix vulnerability 6
- SIPROTEC 7SD686: update to firmware V4.05 [4] or higher to fix vulnerability 2 and 6

Siemens is preparing fixes for the remaining vulnerabilities and recommends the following mitigations in the meantime:

- Apply secure substation concept and Defense-in-Depth [5]
- Restrict network access to port 80/TCP and port 50000/UDP

As a general security measure Siemens recommends to protect network access with appropriate mechanisms [6] (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.

ADDITIONAL RESOURCES

[1] The firmware updates for EN100 communication module firmware variants can be downloaded here: https://support.industry.siemens.com/cs/us/en/view/109745821

[2] The firmware update for SIPROTEC Merging Unit 6MU80 can be obtained by contacting the Siemens hotline at: support.energy@siemens.com

[3] The firmware updates for SIPROTEC 7SJ66 can be obtained here: https://support.industry.siemens.com/cs/gb/en/view/109743555

[4] The firmware updates for SIPROTEC 7SJ686, 7UT686, and 7SD686 can be obtained from the following webpages:
For 7SJ686:
http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=51
For 7UT686:
http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=68
For 7SD686:
http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=64

[5] Recommended security guidelines to Secure Substation:
https://www.siemens.com/gridsecurity
(go to “Downloads” side bar → “Manuals”)

[6] 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 (2017-07-04): Publication Date
V1.1 (2017-07-18): Added update for DNP3 TCP
V1.2 (2017-07-25): Added update for IEC 104
V1.3 (2017-09-07): Added update for Modbus TCP
V1.4 (2017-10-09): Corrected “Affected Products” and added update for SIPROTEC 7SJ686
V1.5 (2017-11-30): Added update for 7SD686
V1.6 (2017-12-22): Added update for 7UT686

DISCLAIMER

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