SSA-547990: Information Disclosure Vulnerabilities in SIPROTEC 4 and SIPROTEC Compact

Publication Date 2016-05-19
Last Update 2016-06-30
Current Version V1.1
CVSS Overall Score 3.9

SUMMARY

Information disclosure vulnerabilities in SIPROTEC 4 and SIPROTEC Compact devices could allow an attacker to extract sensitive device information under certain conditions.

Siemens has released firmware updates for EN100 Ethernet module included in SIPROTEC 4 and SIPROTEC Compact devices. Siemens has also released a firmware update for SIPROTEC Compact 7SJ80 with Ethernet Service Interface on Port A. For remaining affected devices, countermeasures are recommended. Siemens will update this advisory when new information becomes available.

AFFECTED PRODUCTS

- EN100 Ethernet module included in SIPROTEC 4 and SIPROTEC Compact:
  EN100 version V4.26 or lower
- SIPROTEC Compact models with Ethernet Service Interface on Port A
  7SJ80: Firmware version V4.75 or lower;
  7SD80, 7RW80, 7SJ81, 7SK81: All firmware 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 Ethernet modules are used for enabling IEC 61850 communication with electrical/optical 100 Mbit interfaces for SIPROTEC 4 and SIPROTEC Compact devices.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (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 defined by the customer to accomplish final scoring.

Vulnerability 1 (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 5.0
CVSS Temporal Score 3.9
CVSS Overall Score 3.9 (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Vulnerability 2 (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. This vulnerability only affects EN100 Ethernet module included in SIPROTEC 4 and SIPROTEC Compact devices.

CVSS Base Score	5.0
CVSS Temporal Score	3.9
CVSS Overall Score	3.9 (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Mitigating Factors

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

SOLUTION

Siemens provides firmware update V4.27 for EN100 module included in SIPROTEC 4 and SIPROTEC Compact to fix the vulnerabilities [1, 2].

For SIPROTEC Compact 7SJ80 with Ethernet Service Interface on Port A, Siemens provides firmware update V4.76 [3].

For remaining affected products Siemens 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:

- Aleksandr Bersenev from HackerDom team for coordinated disclosure of vulnerability 1.
- Pavel Toporkov from Kaspersky Lab for coordinated disclosure of vulnerability 2.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for coordination efforts.

ADDITIONAL RESOURCES

[1] The firmware update for SIPROTEC 4 can be obtained from the SIPROTEC 4 downloads area: http://www.siemens.com/downloads/siprotec-4
(click on the plus sign next to the respective model → “Firmware and Device Drivers” → “Communication Protocols – IEC 61850” → “Update EN100 V4.27 for all devices over the EN100 interface” or “Update EN100 V4.27 for all devices over the front interface”)

[2] The firmware update for SIPROTEC Compact with EN100 module can be obtained here: http://www.siemens.com/downloads/siprotec-compact
(click on the plus sign next to the respective model → “Firmware and Device Drivers” → “Communication Protocols – IEC 61850” → “Update EN100 V4.27 over the EN100 interface” or “Update EN100 V4.27 over the front interface”)

[3] The firmware update for SIPROTEC Compact 7SJ80 can be obtained here: http://www.siemens.com/downloads/siprotec-compact
(click on the plus sign next to 7SJ80 → “Firmware and Device Drivers” → “Firmware” → “Setup_7SJ80x_04.76.01”)

[4] Recommended security guidelines to Secure Substation: http://www.siemens.com/gridsecurity
(go to “Cyber Security General Downloads” → “Manuals”)

[5] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-05-19):	Publication Date
V1.1 (2016-06-30):	Added update information for SIPROTEC Compact 7SJ80; removed SIPROTEC Compact 7SK80 from Affected Products

DISCLAIMER