

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

Publication Date: 2017-07-04  
 Last Update: 2018-03-15  
 Current Version: V1.7  
 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 AND SOLUTION

Affected Product and Versions	Remediation
Firmware variant PROFINET IO for EN100 Ethernet module: All versions < V1.04.01	Install V1.04.01 <a href="https://support.industry.siemens.com/cs/us/en/view/109745821">https://support.industry.siemens.com/cs/us/en/view/109745821</a>
Firmware variant Modbus TCP for EN100 Ethernet module: All versions < V1.11.00	Update to V1.11.00 <a href="https://support.industry.siemens.com/cs/us/en/view/109745821">https://support.industry.siemens.com/cs/us/en/view/109745821</a>
Firmware variant DNP3 TCP for EN100 Ethernet module: All versions < V1.03	Install V1.03 <a href="https://support.industry.siemens.com/cs/us/en/view/109745821">https://support.industry.siemens.com/cs/us/en/view/109745821</a>
Firmware variant IEC 104 for EN100 Ethernet module: All versions < V1.21	Install V1.21 <a href="https://support.industry.siemens.com/cs/us/en/view/109745821">https://support.industry.siemens.com/cs/us/en/view/109745821</a>
EN100 Ethernet module included in SIPROTEC Merging Unit 6MU80: All versions < 1.02.02	Install V1.02.02 Please contact the Siemens hotline at <a href="mailto:support.energy@siemens.com">support.energy@siemens.com</a>
SIPROTEC 7SJ686: All versions < V 4.83 only affected by CVE-2016-4784	Install V 4.83 <a href="http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=51">http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=51</a>
SIPROTEC 7SJ686: All versions < V 4.87 only affected by CVE-2016-7114	Siemens is preparing fixes, please see "Mitigations and workarounds" in the meantime. <a href="http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=51">http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=51</a>
SIPROTEC 7UT686: All versions < V 4.01 only affected by CVE-2016-4784	Install V 4.01 <a href="http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=68">http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=68</a>

SIPROTEC 7UT686: All versions < V 4.02 only affected by CVE-2016-7114	Install V4.02 <a href="http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=68">http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=68</a>
SIPROTEC 7SD686: All versions < V 4.03 only affected by CVE-2016-4784	Install V 4.03 <a href="http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=64">http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=64</a>
SIPROTEC 7SD686: All versions < V 4.05 only affected by CVE-2016-7114	Install V4.05 <a href="http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=64">http://www.siemensenergysector.com/ProductRelatedDown.aspx?ProductId=64</a>
SIPROTEC 7SJ66: All versions < V 4.20 only affected by CVE-2016-4784	Install V 4.20 <a href="https://support.industry.siemens.com/cs/gb/en/view/109743555">https://support.industry.siemens.com/cs/gb/en/view/109743555</a>
SIPROTEC 7SJ66: All versions < V 4.30 only affected by CVE-2016-7114	Install V 4.30 <a href="https://support.industry.siemens.com/cs/us/en/view/109743555">https://support.industry.siemens.com/cs/us/en/view/109743555</a>

## **WORKAROUNDS AND MITIGATIONS**

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Apply secure substation concept and Defense-in-Depth (see <https://www.siemens.com/gridsecurity>)
- Restrict network access to port 80/TCP and port 50000/UDP

## **GENERAL SECURITY RECOMMENDATIONS**

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 in order to run the devices in a protected IT environment.

Recommended security guidelines to Secure Substations can be found at:

<https://www.siemens.com/gridsecurity>

## **PRODUCT 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 process communication and either IEC 61850, PROFINET IO, Modbus TCP, DNP3 TCP or IEC 104 communication with electrical/optical 100 Mbit interfaces for SIPROTEC 4, SIPROTEC Compact and Reyrolle 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.

## **VULNERABILITY CLASSIFICATION**

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (<https://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 (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 v3.0 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 (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 v3.0 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 (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 SIPROTEC4 and SIPROTEC Compact devices.

CVSS v3.0 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 (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 v3.0 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

Vulnerability (CVE-2016-7113)

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

CVSS v3.0 Base Score 5.3  
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Vulnerability (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 v3.0 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

**ADDITIONAL INFORMATION**

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  
V1.7 (2018-03-15): Added update for 7SJ66

## **TERMS OF USE**

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website ([https://www.siemens.com/terms\\_of\\_use](https://www.siemens.com/terms_of_use), hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.