SSA-630413: Vulnerabilities in SIPROTEC 4 and SIPROTEC Compact

Publication Date 2016-09-05
Last Update 2016-09-05
Current Version V1.0
CVSS v3.0 Base Score 5.3

SUMMARY

The latest firmware update for in SIPROTEC 4 and SIPROTEC Compact devices fixes multiple vulnerabilities. The most severe of these vulnerabilities could allow unauthorized users to access the administrative web application.

AFFECTED PRODUCTS

EN100 Ethernet module (as optional for SIPROTEC 4 and SIPROTEC Compact): All versions < V4.29

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

Vulnerability 2 (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 v3.0 Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Vulnerability 3 (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 v3.0 Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

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 firmware update V4.29 for EN100 modules included in SIPROTEC 4 and SIPROTEC Compact to fix the vulnerability [1, 2]. Siemens recommends customers to update to the latest firmware version.

As a general security measure Siemens recommends to protect network access with appropriate mechanisms [3] (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:

- Kirill Nesterov and Anatoly Katushin from Kaspersky Lab for reporting vulnerabilities 1 and 2.

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 à <product type> à Firmware and Device Drivers à Communication Protocols - IEC 61850 à Update EN100 V4.29

[2] The firmware update for SIPROTEC Compact with EN100 module can be obtained here: http://www.siemens.com/downloads/siprotec-compact à <product type> à Firmware and Device Drivers à Communication Protocols - IEC 61850 à Firmware update EN100 V4.29

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

[4] 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 (2016-09-05): Publication Date

DISCLAIMER