SSA-732541: Denial-of-Service Vulnerability in SIPROTEC 4

Publication Date 2015-07-17
Last Update 2017-06-12
Current Version V1.1
CVSS Overall Score 6.8

Summary

The latest firmware updates for the affected devices resolve a vulnerability which could allow attackers to perform a denial-of-service attack under certain conditions.

AFFECTED PRODUCTS

- SIPROTEC 4 and SIPROTEC Compact product families: All devices where the Ethernet module EN100 with version V4.24 or lower is included.

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 module is used for enabling IEC 61850 communication with electrical/optical 100 Mbit interface for SIPROTEC 4 and SIPROTEC Compact devices.

Detailed information about the vulnerability 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 Description (CVE-2015-5374)

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

CVSS Base Score	7.8
CVSS Temporal Score	6.8
CVSS Overall Score	6.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:H/RL:OF/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 firmware update V4.25 and subsequent cumulative updates for the EN100 module to fix the vulnerability [1, 2].

As a general security measure Siemens strongly recommends to keep the firmware up-to-date and to protect network access with appropriate mechanisms [3]. It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks Victor Nikitin from i-Grids LLC Russia for coordinated disclosure of the vulnerability.

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
(expand entry for SIPROTEC 4 device type e.g. 7SJ64 à "Firmware and Device Drivers" à "Communication Protocols - IEC 61850" à "Update EN100 V4.29 for all devices over the EN100 interface")

[2] The firmware update for SIPROTEC Compact can be obtained here:
http://www.siemens.com/downloads/siprotec-compact
(expand entry for SIPROTEC Compact device type e.g. 7SJ80 à "Firmware and Device Drivers" à "Communication Protocols - IEC 61850" à "Firmware update V4.29 over the EN100 interface")

[3] Recommended security guidelines to Secure Substation:
http://www.siemens.com/gridsecurity
(go to "Downloads" side bar à "Manuals")

[4] 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 (2015-07-17):	Publication Date
V1.1 (2017-06-12):	Updated download path for SIPROTEC 4 and Compact; Adjusted CVSS Score and Vector;

DISCLAIMER