SSA-203306: Password Vulnerabilities in SIPROTEC 4 and SIPROTEC Compact Relay Families

Publication Date: 2018-03-08
Last Update: 2018-04-17
Current Version: V1.2
CVSS v3.0 Base Score: 7.5

SUMMARY

SIPROTEC 4 and SIPROTEC Compact devices could allow access authorization passwords to be reconstructed or overwritten via engineering mechanisms that involve DIGSI 4 and EN100 Ethernet communication modules.

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

For customers who are currently using the discontinued EN100-E or EN100-O modules, Siemens recommends to upgrade to EN100-E+ or EN100-O+ modules in order to apply the firmware updates.

Affected Product and Versions	Remediation
DIGSI 4: All versions < V4.92	Update to V4.92 https://support.industry.siemens.com/cs/ww/en/view/109740980
EN100 Ethernet module IEC 61850 variant: All versions < V4.30	Update to V4.30 and configure DIGSI 4 connection password https://support.industry.siemens.com/cs/us/en/view/109745821
EN100 Ethernet module PROFINET IO variant: All versions	See recommendations from section Workarounds and Mitigations
EN100 Ethernet module Modbus TCP variant: All versions	See recommendations from section Workarounds and Mitigations
EN100 Ethernet module DNP3 variant: All versions < V1.04	Update to V4.30 and configure DIGSI 4 connection password https://support.industry.siemens.com/cs/us/en/view/109745821
EN100 Ethernet module IEC 104 variant: All versions	See recommendations from section Workarounds and Mitigations
SIPROTEC Compact 7SJ80: All versions < V4.77 only affected by CVE-2018-4839	Update to V4.77 https://support.industry.siemens.com/cs/us/en/view/109742699
SIPROTEC Compact 7SK80: All versions < V4.77 only affected by CVE-2018-4839	Update to V4.77 https://support.industry.siemens.com/cs/us/en/view/109742712

SIPROTEC 4 7SJ66: All versions < V4.30 only affected by CVE-2018-4839	Update to V4.30 https://support.industry.siemens.com/cs/us/en/view/109743555
Other SIPROTEC Compact relays: All versions only affected by CVE-2018-4839	See recommendations from section Workarounds and Mitigations
Other SIPROTEC 4 relays: All versions only affected by CVE-2018-4839	See recommendations from section Workarounds and Mitigations

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)

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.

DIGSI 4 is the operation and configuration software for SIPROTEC 4 and SIPROTEC Compact protection devices.

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-2018-4839

An attacker with local access to the engineering system or in a privileged network position and able to obtain certain network traffic could possibly reconstruct access authorization passwords.

CVSS v3.0 Base Score	4.0
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-4840

The device engineering mechanism allows an unauthenticated remote user to upload a modified device configuration overwriting access authorization passwords.

CVSS v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Ilya Karpov and Dmitry Sklyarov from Positive Technologies for coordinated disclosure

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 (2018-03-08):	Publication Date
V1.1 (2018-03-08):	Corrected product name SIPROTEC 4 7SJ66
V1.2 (2018-04-17):	Added update for DNP3 TCP

TERMS OF USE