

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

Publication Date: 2018-03-08
Last Update: 2021-07-13
Current Version: V1.5
CVSS v3.1 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, and recommends specific countermeasures for the remaining products.

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 DNP3 variant: All versions < V1.05.00	Update to V1.05.00 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
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 Modbus TCP variant: All versions	See recommendations from section Workarounds and Mitigations
EN100 Ethernet module PROFINET IO variant: All versions	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
Other SIPROTEC Compact relays: All versions only affected by CVE-2018-4839	See recommendations from section Workarounds and Mitigations

SIPROTEC 4 7SD80: All versions < V4.70 only affected by CVE-2018-4839	Update to V4.70 https://support.industry.siemens.com/cs/us/en/view/109742758
SIPROTEC 4 7SJ61: All versions < V4.96 only affected by CVE-2018-4839	Update to V4.96 https://support.industry.siemens.com/cs/us/en/view/109743551
SIPROTEC 4 7SJ62: All versions < V4.96 only affected by CVE-2018-4839	Update to V4.96 https://support.industry.siemens.com/cs/us/en/view/109743551
SIPROTEC 4 7SJ64: All versions < V4.96 only affected by CVE-2018-4839	Update to V4.96 https://support.industry.siemens.com/cs/us/en/view/109743551
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
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

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>) or contact customer care to find specific solutions.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

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 Digital Grid Products can be found at:

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

PRODUCT DESCRIPTION

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

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 on either IEC 61850, PROFINET IO, Modbus TCP, DNP3 TCP or IEC 104 protocols via electrical/optical 100 Mbit interfaces on SIPROTEC 4, SIPROTEC Compact, Reyrolle and SWT3000 devices.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (<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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: <https://cwe.mitre.org/>.

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 v3.1 Base Score	4.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-326: Inadequate Encryption Strength

Vulnerability CVE-2018-4840

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

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

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 security 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
V1.3 (2018-05-15): Added update for 7SD80
V1.4 (2019-03-12): Added updates for 7SJ61, 7SJ62 and 7SJ64, and recommendation to contact customer care for products without solution
V1.5 (2021-07-13): Corrected update version for DNP3

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, 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.