SSA-159860: Access Control Vulnerability in IEC 61850 system configurator, DIGSI 5, DIGSI 4, SICAM PAS/PQS, SICAM PQ Analyzer, and SICAM SCC

Publication Date:	2018-06-26
Last Update:	2018-11-13
Current Version:	V1.1
CVSS v3.0 Base Score:	4.2

SUMMARY

IEC 61850 system configurator, DIGSI 5, DIGSI 4, SICAM PAS/PQS, SICAM PQ Analyzer, and SICAM SCC products are affected by a security vulnerability which could allow an attacker to either exfiltrate limited data from the system or to execute code with operating system user permissions.

Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
IEC 61850 system configurator: All versions < V5.80	Update to V5.80 https://support.industry.siemens.com/cs/ww/en/view/109740546
DIGSI 5 (affected as IEC 61850 system configurator is incorporated): All versions < V7.80	Uninstall IEC 61850 system configurator or update to V7.80 https://support.industry.siemens.com/cs/ww/en/view/109758531
DIGSI 4: All versions < V4.93	Update to V4.93 https://support.industry.siemens.com/cs/ww/en/view/109740980
SICAM PAS/PQS: All versions < V8.11	Update to V8.11 https://support.industry.siemens.com/cs/us/en/view/109757831
SICAM PQ Analyzer: All versions < V3.11	Update to V3.11 https://support.industry.siemens.com/cs/us/en/view/109757833
SICAM SCC: All versions < V9.02 HF3	Update to V9.02 HF3 https://support.industry.siemens.com/cs/ww/en/view/109745469

WORKAROUNDS AND MITIGATIONS

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

- Change firewall configuration to restrict access to port 4884/TCP, 5885/TCP or 5886/TCP to localhost (depending on the affected product in use).

- Follow Secure Substations security guidelines 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

The IEC 61850 system configurator is a manufacturer-neutral solution for the interoperable engineering of IEC 61850 products and systems.

DIGSI 5 is the operation and configuration software for SIPROTEC 5 protection devices.

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

SICAM PAS/PQS is an energy automation solution for operating an electrical substation with its devices.

SICAM PQ Analyzer is a power quality system software that provides options to evaluate archived PQ measuring data and fault records.

SICAM SCC is a process and visualization system for energy automation solutions.

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-2018-4858

A service of the affected products listening on all of the host's network interfaces on either port 4884/TCP, 5885/TCP, or port 5886/TCP could allow an attacker to either exfiltrate limited data from the system or to execute code with Microsoft Windows user permissions.

Successful exploitation requires an attacker to be able to send a specially crafted network request to the vulnerable service and a user interacting with the service's client application on the host. In order to execute arbitrary code with Microsoft Windows user permissions, an attacker must be able to plant the code in advance on the host by other means. The vulnerability has limited impact to confidentiality and integrity of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.

CVSS v3.0 Base Score	4.2
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Chris Bellows and HD Moore from Atredis Partners for coordinated disclosure
- Austin Scott from San Diego Gas and Electric 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 (2018-06-26):	Publication Date
V1.1 (2018-11-13):	Updates for DIGSI 4 and SICAM SCC

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.