SSA-496292: Remote Code Execution Vulnerability in POWER METER SICAM Q100

Publication Date: 2021-12-14
Last Update: 2021-12-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.1

SUMMARY

POWER METER SICAM Q100 contains a vulnerability that could allow an attacker to remotely execute code.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
POWER METER SICAM Q100 (7KG9501-0AA01-0AA1): All versions < V2.41	Update to V2.41 or later version https://support.industry.siemens.com/cs/ww/en/view/109743524 See further recommendations from section Workarounds and Mitigations
POWER METER SICAM Q100 (7KG9501-0AA01-2AA1): All versions < V2.41	Update to V2.41 or later version https://support.industry.siemens.com/cs/ww/en/view/109743524 See further recommendations from section Workarounds and Mitigations
POWER METER SICAM Q100 (7KG9501-0AA31-0AA1): All versions < V2.41	Update to V2.41 or later version https://support.industry.siemens.com/cs/ww/en/view/109743524 See further recommendations from section Workarounds and Mitigations
POWER METER SICAM Q100 (7KG9501-0AA31-2AA1): All versions < V2.41	Update to V2.41 or later version https://support.industry.siemens.com/cs/ww/en/view/109743524 See further 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:

- Restrict access to the web server e.g. with a firewall and ensure that the privileged accounts are protected by strong passwords.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial

Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

The POWER METER SICAM Q100 device is a multifunctional device for detecting, reporting, and analyzing measured values and events.

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-2021-44165

The affected firmware contains a buffer overflow vulnerability in the web application that could allow a remote attacker with engineer or admin priviliges to potentially perform remote code execution.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Messner from Siemens Energy for reporting the vulnerability

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 (2021-12-14): Publication Date

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.