

SSA-570294: Multiple Vulnerabilities in SICAM Q100 Before V2.50

Publication Date: 2022-11-08
Last Update: 2024-01-09
Current Version: V1.1
CVSS v3.1 Base Score: 9.9

SUMMARY

SICAM Q100 devices contain multiple vulnerabilities that could allow an attacker to take over the session of a logged in user or to inject custom 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 < V2.50	Update to V2.50 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 < V2.50	Update to V2.50 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 < V2.50	Update to V2.50 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 < V2.50	Update to V2.50 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 port 443/tcp to trusted IP addresses only

Product-specific remediations or mitigations can be found in the section [Affected Products and Solution](#). Please follow the [General Security Recommendations](#).

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 can be found at: <https://www.siemens.com/gridsecurity>

PRODUCT DESCRIPTION

POWER METER SICAM Q100 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-2022-43398

Affected devices do not renew the session cookie after login/logout and also accept user defined session cookies. An attacker could overwrite the stored session cookie of a user. After the victim logged in, the attacker is given access to the user's account through the activated session.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-384: Session Fixation

Vulnerability CVE-2022-43439

Affected devices do not properly validate the Language-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2022-43545

Affected devices do not properly validate the RecordType-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.

CVSS v3.1 Base Score 9.9
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2022-43546

Affected devices do not properly validate the EndTime-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.

CVSS v3.1 Base Score 9.9
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Michael Messner from Siemens Energy for reporting the vulnerabilities

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 (2022-11-08): Publication Date
V1.1 (2024-01-09): Added legacy Q100 device models (-0AA1) which are also affected and provide the same fix version

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.