SSA-480095: Vulnerabilities in the Web Interface of SICAM Q100 Devices before V2.60

Publication Date: 2023-12-12
Last Update: 2024-01-09
Current Version: V1.1
CVSS v3.1 Base Score: 5.5

SUMMARY

The web server of SICAM Q100 devices, versions before V2.60, contains a Cross Site Request Forgery (CSRF) vulnerability and is missing cookie protection flags. This could allow an attacker to perform arbitrary actions on the device on behalf of a legitimate user, or impersonate that user.

Siemens has released new versions 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 < V2.60	Update to V2.60 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 < V2.60	Update to V2.60 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 < V2.60	Update to V2.60 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 < V2.60	Update to V2.60 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:

- CVE-2023-31238: Restrict access to port 443/tcp to trusted IP addresses only
- CVE-2023-30901: Do not access links from untrusted sources while logged in at affected devices

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-2023-30901

The web interface of the affected devices are vulnerable to Cross-Site Request Forgery attacks. By tricking an authenticated victim user to click a malicious link, an attacker could perform arbitrary actions on the device on behalf of the victim user.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability CVE-2023-31238

Affected devices are missing cookie protection flags when using the default settings. An attacker who gains access to a session token can use it to impersonate a legitimate application user.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

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 (2023-12-12):	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