SSA-165073: Multiple Vulnerabilities in the Webinterface of SICAM P850 and SICAM P855 Devices

Publication Date: 2022-05-10
Last Update: 2022-05-10
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Multiple vulnerabilities were identified in the webserver of SICAM P850 and SICAM P855 devices. These include unauthenticated access to web-interface functionality, missing HTTPS or impersonation as well as cross-site scripting related vulnerabilities.

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
SICAM P850 (7KG8500-0AA00-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8500-0AA00-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8500-0AA10-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8500-0AA10-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8500-0AA30-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8500-0AA30-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations

SICAM P850 (7KG8501-0AA01-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA01-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA02-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA02-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA11-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA11-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA12-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA12-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA31-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA31-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations

SICAM P850 (7KG8501-0AA32-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P850 (7KG8501-0AA32-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743594/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8550-0AA00-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8550-0AA00-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8550-0AA10-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8550-0AA10-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8550-0AA30-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8550-0AA30-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA01-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA01-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations

SICAM P855 (7KG8551-0AA02-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA02-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA11-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA11-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA12-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA12-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA31-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA31-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA32-0AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ See further recommendations from section Workarounds and Mitigations
SICAM P855 (7KG8551-0AA32-2AA0): All versions < V3.00	Update to V3.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109743621/ 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:

- Do not access links from untrusted sources while logged in at SICAM P850 or SICAM P855 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

The SICAM P850 multifunctional measuring device is used for acquisition, visualization, evaluation and transmission of electrical measured variables such as alternating current, alternating voltage, frequency, power, harmonics etc.

The SICAM P855 multifunctional device is used to collect, display and transmit measured electrical variables such as AC current, AC voltage, power types, harmonics, etc. The measurands and events are collected and processed according to the Power Quality Standard IEC 61000-4-30.

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-2022-29872

Affected devices do not properly validate parameters of POST requests. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-141: Improper Neutralization of Parameter/Argument Delimiters

Vulnerability CVE-2022-29873

Affected devices do not properly validate parameters of certain GET and POST requests. This could allow an unauthenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-141: Improper Neutralization of Parameter/Argument Delimiters

Vulnerability CVE-2022-29874

Affected devices do not encrypt web traffic with clients but communicate in cleartext via HTTP. This could allow an unauthenticated attacker to capture the traffic and interfere with the functionality of the device.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

Vulnerability CVE-2022-29876

Affected devices do not properly handle the input of a GET request parameter. The provided argument is directly reflected in the web server response. This could allow an unauthenticated attacker to perform reflected XSS attacks.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)

Vulnerability CVE-2022-29877

Affected devices allow unauthenticated access to the web interface configuration area. This could allow an attacker to extract internal configuration details or to reconfigure network settings. However, the reconfigured settings cannot be activated unless the role of an authenticated administrator user.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2022-29878

Affected devices use a limited range for challenges that are sent during the unencrypted challenge-response communication. An unauthenticated attacker could capture a valid challenge-response pair generated by a legitimate user, and request the webpage repeatedly to wait for the same challenge to reappear for which the correct response is known. This could allow the attacker to access the management interface of the device.

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-294: Authentication Bypass by Capture-replay

Vulnerability CVE-2022-29879

The web based management interface of affected devices does not employ special access protection for certain internal developer views. This could allow authenticated users to access critical device information.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2022-29880

Affected devices do not properly validate input in the configuration interface. This could allow an authenticated attacker to place persistent XSS attacks to perform arbitrary actions in the name of a logged user which accesses the affected views.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)

Vulnerability CVE-2022-29881

The web based management interface of affected devices does not employ special access protection for certain internal developer views. This could allow unauthenticated users to extract internal configuration details.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2022-29882

Affected devices do not handle uploaded files correctly. An unauthenticated attacker could take advantage of this situation to store an XSS attack, which could - when a legitimate user accesses the error logs - perform arbitrary actions in the name of the user.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)

Vulnerability CVE-2022-29883

Affected devices do not restrict unauthenticated access to certain pages of the web interface. This could allow an attacker to delete log files without authentication.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

ACKNOWLEDGMENTS

Siemens thanks the following parties for their 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 (2022-05-10): Publication Date

TERMS OF USE