

## **SSA-572005: Vulnerabilities in the Web Server of SICAM P850 and SICAM P855 Devices**

Publication Date: 2022-10-11  
 Last Update: 2022-12-13  
 Current Version: V1.1  
 CVSS v3.1 Base Score: 9.8

### **SUMMARY**

Session fixation and incorrect parameter parsing vulnerabilities were identified in the web server of SICAM P850 and SICAM P855 devices.

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

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
SICAM P850 (7KG8500-0AA00-0AA0); All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8500-0AA00-2AA0); All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8500-0AA10-0AA0); All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8500-0AA10-2AA0); All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8500-0AA30-0AA0); All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8500-0AA30-2AA0); All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

SICAM P850 (7KG8501-0AA01-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA01-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA02-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA02-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA11-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA11-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA12-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA12-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA31-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA31-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

SICAM P850 (7KG8501-0AA32-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P850 (7KG8501-0AA32-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743594/">https://support.industry.siemens.com/cs/ww/en/view/109743594/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8550-0AA00-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8550-0AA00-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8550-0AA10-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8550-0AA10-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8550-0AA30-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8550-0AA30-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA01-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA01-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

SICAM P855 (7KG8551-0AA02-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA02-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA11-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA11-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA12-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA12-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA31-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA31-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA32-0AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM P855 (7KG8551-0AA32-2AA0): All versions < V3.10	Update to V3.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109743621/">https://support.industry.siemens.com/cs/ww/en/view/109743621/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

## **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-2022-40226**

Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login.

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-2022-41665**

Affected devices do not properly validate the parameter of a specific GET request. 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

## **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 (2022-10-11):      Publication Date  
V1.1 (2022-12-13):      Corrected description for CVE-2022-41665; corrected CVSS score for CVE-2022-40226

## **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](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.