

Forum:[Hack Forums](#)

Thread: [Siemens SICAM P850 family and SICAM P855 family](#)

Stanley - November 23, 2025, 11:20 pm

Siemens SICAM P850 family and SICAM P855 family

As of January 10, 2023, CISA will no longer be updating ICS security advisories for Siemens product vulnerabilities beyond the initial advisory. For the most up-to-date information on vulnerabilities in this advisory, please see Siemens' ProductCERT Security Advisories (CERT Services | Services | Siemens Global).View CSAF

1. EXECUTIVE SUMMARY

CVSS v3 5.5

ATTENTION: Exploitable remotely/low attack complexity

Vendor: Siemens

Equipment: SICAM P850 family and SICAM P855 family

Vulnerabilities: Cross-Site Request Forgery (CSRF), Incorrect Permission Assignment for Critical Resource

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to perform arbitrary actions on the device on behalf of a legitimate user, or impersonate that user.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Siemens reports that the following products are affected:

SICAM P850 (7KG8500-0AA00-0AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA02-2AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA11-0AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA11-2AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA12-0AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA12-2AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA31-0AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA31-2AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA32-0AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA32-2AA0): Versions prior to 3.11
SICAM P855 (7KG8550-0AA00-0AA0): Versions prior to 3.11
SICAM P850 (7KG8500-0AA00-2AA0): Versions prior to 3.11
SICAM P855 (7KG8550-0AA00-2AA0): Versions prior to 3.11
SICAM P855 (7KG8550-0AA10-0AA0): Versions prior to 3.11
SICAM P855 (7KG8550-0AA10-2AA0): Versions prior to 3.11
SICAM P855 (7KG8550-0AA30-0AA0): Versions prior to 3.11
SICAM P855 (7KG8550-0AA30-2AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA01-0AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA01-2AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA02-0AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA02-2AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA11-0AA0): Versions prior to 3.11
SICAM P850 (7KG8500-0AA10-0AA0): Versions prior to 3.11

SICAM P855 (7KG8551-0AA11-2AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA12-0AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA12-2AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA31-0AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA31-2AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA32-0AA0): Versions prior to 3.11
SICAM P855 (7KG8551-0AA32-2AA0): Versions prior to 3.11
SICAM P850 (7KG8500-0AA10-2AA0): Versions prior to 3.11
SICAM P850 (7KG8500-0AA30-0AA0): Versions prior to 3.11
SICAM P850 (7KG8500-0AA30-2AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA01-0AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA01-2AA0): Versions prior to 3.11
SICAM P850 (7KG8501-0AA02-0AA0): Versions prior to 3.11

3.2 VULNERABILITY OVERVIEW

3.2.1 CROSS-SITE REQUEST FORGERY (CSRF) CWE-352

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.

CVE-2023-30901 has been assigned to this vulnerability. A CVSS v3.1 base score of 4.3 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).

3.2.2 INCORRECT PERMISSION ASSIGNMENT FOR CRITICAL RESOURCE CWE-732

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.

CVE-2023-31238 has been assigned to this vulnerability. A CVSS v3.1 base score of 5.5 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Energy

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: Germany

3.4 RESEARCHER

Siemens ProductCERT reported these vulnerabilities to CISA.

4. MITIGATIONS

Siemens has identified the following specific workarounds and mitigations users can apply to reduce risk:

Update to V3.11 or later version

(CVE-2023-30901) All affected products: Do not access links from untrusted sources while logged in at affected devices

(CVE-2023-31238) All affected products: Restrict access to port 443/tcp to trusted IP addresses only

As a general security measure, Siemens recommends protecting network access to devices with appropriate mechanisms. To operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens' operational guidelines for industrial security and following recommendations in the product manuals.

Additional information on industrial security by Siemens can be found on the Siemens industrial security webpage

For more information see the associated Siemens security advisory SSA-201498 in HTML and CSAF.

CISA recommends users take defensive measures to minimize the risk of exploitation of these

vulnerabilities, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs). Recognize VPNs may have vulnerabilities, should be updated to the most recent version available, and are only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on [cisa.gov](https://www.cisa.gov). Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at [cisa.gov](https://www.cisa.gov) in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

5. UPDATE HISTORY

November 13, 2025: Initial Republication of Siemens ProductCERT SSA-201498

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-11>