SSA-631336: Multiple Web Server Vulnerabilities in SICAM GridEdge Software

Publication Date: 2022-06-14
Last Update: 2022-06-14
Current Version: V1.0
CVSS v3.1 Base Score: 10.0

SUMMARY

Multiple vulnerabilities were identified in the webserver of the SICAM GridEdge application which includes missing authentication for critical API functions, absent cross-origin resource sharing restrictions and access to credentials.

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 GridEdge Essential ARM (6MD7881-2AA30): All versions < V2.6.6	Update to V2.6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109780559/ See further recommendations from section Workarounds and Mitigations
SICAM GridEdge Essential Intel (6MD7881-2AA40): All versions < V2.6.6	Update to V2.6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109780559/ See further recommendations from section Workarounds and Mitigations
SICAM GridEdge Essential with GDS ARM (6MD7881-2AA10): All versions < V2.6.6	Update to V2.6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109780559/ See further recommendations from section Workarounds and Mitigations
SICAM GridEdge Essential with GDS Intel (6MD7881-2AA20): All versions < V2.6.6	Update to V2.6.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109780559/ 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:

- Limit access to port 8900/tcp to trusted users and systems 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

SICAM GridEdge enables your existing IEC61850 equipment with IoT functionality using just a few clicks. Based on international standards (MQTT, OPC UA Pub/Sub (IEC 62451), IEC61850) data collected from your equipment is transmitted to well-known cloud platforms Siemens MindSphere, Microsoft Azure and to self-hosted platforms. SICAM GridEdge creates a multi-layered communication architecture, where the substation IEDs are capable of ingesting local huge data streams and only transmit relevant pre-processed data into the cloud.

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-2022-30228

The affected software does not apply cross-origin resource sharing (CORS) restrictions for critical operations. In case an attacker tricks a legitimate user into accessing a special resource a malicious request could be executed.

CVSS v3.1 Base Score	9.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-346: Origin Validation Error

Vulnerability CVE-2022-30229

The affected software does not require authenticated access for privileged functions. This could allow an unauthenticated attacker to change data of an user, such as credentials, in case that user's id is known.

CVSS v3.1 Base Score	9.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2022-30230

The affected software does not require authenticated access for privileged functions. This could allow an unauthenticated attacker to create a new user with administrative permissions.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2022-30231

The affected software discloses password hashes of other users upon request. This could allow an authenticated user to retrieve another users password hash.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Abian Blome 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 (2022-06-14): Publication Date

TERMS OF USE