SSA-225578: Improper Access Control in SICAM GridEdge

Publication Date: 2022-07-12
Last Update: 2022-07-12
Current Version: V1.0
CVSS v3.1 Base Score: 6.3

SUMMARY

The SICAM GridEdge software contains a improper access control vulnerability. This could allow persons with local access to the host system to inject an SSH key.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM GridEdge Essential ARM (6MD7881-2AA30): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SICAM GridEdge Essential Intel (6MD7881-2AA40): All versions < V2.7.3	Update to V2.7.3 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SICAM GridEdge Essential with GDS Intel (6MD7881-2AA20): All versions < V2.7.3	Update to V2.7.3 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:

- Restrict physical access to the device and limit access to the ssh port (22/tcp) to trusted IP addresses if possible.

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-2022-34464

Affected software uses an improperly protected file to import SSH keys. Attackers with access to the filesystem of the host on which SICAM GridEdge runs, are able to inject a custom SSH key to that file.

CVSS v3.1 Base Score	6.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-668: Exposure of Resource to Wrong Sphere

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 (2022-07-12):   Publication Date

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, 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.