SSA-305120: Vulnerabilities in SICAM MMU, SICAM T and SICAM SGU

Publication Date: 2020-07-14
Last Update: 2020-07-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

SICAM MMU, SICAM T and the discontinued SICAM SGU devices are affected by multiple security vulnerabilities which could allow an attacker to perform a variety of attacks. This may include unauthenticated firmware installation, remote code execution and leakage of confidential data like passwords. Siemens has released updates to introduce authentication to the web application. It is still recommended to implement further mitigations, as most of the vulnerabilities might not be sufficiently mitigated by this.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM MMU: All versions < V2.05	Update to V2.05 to introduce authentication in the web application to mitigate some web application issues. https://support.industry.siemens.com/cs/ww/en/ps/7KG9663-1AA00-1AA0
SICAM SGU: All versions	For RTU applications, Siemens recommends to upgrade the discontinued SICAM SGU devices to SICAM A8000 RTUs.
SICAM T: All versions < V2.18	Update to V2.18 to introduce authentication in the web application to mitigate some web application issues. https://support.industry.siemens.com/cs/ww/en/ps/7KG9661-1AA00-1AA0

WORKAROUNDS AND MITIGATIONS

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

- The firmware updates to SICAM T and SICAM MMU introduce authentication to the web application and remove some unnecessary functionality. The web authentication functionality reduces the risk of access to the device's web application for executing administrative commands by unauthenticated users.
- Due to hardware constraints, encryption is not possible on the devices. Confidential data such as passwords handled by the devices need to be protected on the network by other means, e.g. by VPN.
- The risk for remote code execution and unauthenticated firmware installation can be mitigated by ensuring encryption and authentication between the user and the device, e.g. by VPN.
- Using a modern and up to date browser while accessing the web application might reduce the risk of Cross-Site-Scripting attacks.

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 to Digital Grid Products can be found at:

https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

SICAM T is a digital measurement transducer that allows the measuring of electrical quantities in electrical networks in a single unit. In industries, power plants and substations, transducers are especially used for measurand (e.g. current, voltage, power, phase angle, energy or frequency) assignment into further processing through analog outputs or communication interface for precise control, notification or visualization tasks.

SICAM MMU (Measurement and Monitoring Unit) is a power monitoring device that allows the measuring of electrical quantities in electrical networks in a single unit. In industries, power plants and substations, the SICAM MMU is applied to measure and calculate parameters (e.g.current, voltage, power, phase angle, harmonics and unbalance, energy or frequency) and assign them into further processing and visualization to control center (SCADA, DMS, EMS etc) through IEC 60870-5-104 or automation system over MODBUS TCP Protocols.

SICAM SGU (discontinued) was a smart grid remote terminal unit with communication capabilities for electric utilities and public utility companies. It was intended to be used in particular as an input and output unit for distributed power generation plants and consumers. Distributed energy resources could be controlled and monitored by control centers (CC) or Decentralized Energy Management Systems (DEMS) via the communication interfaces.

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-2020-10037

By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2020-10038

An attacker with access to the device's web server might be able to execute administrative commands without authentication.

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:T/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2020-10039

An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data.

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:T/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-10040

An attacker with local access to the device might be able to retrieve some passwords in clear text.

CVSS v3.1 Base Score	6.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C
CWE	CWE-916: Use of Password Hash With Insufficient Computational Effort

Vulnerability CVE-2020-10041

A stored Cross-Site-Scripting (XSS) vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user.

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:T/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2020-10042

A buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network.

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:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2020-10043

The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:L/E:P/RL:T/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Vulnerability CVE-2020-10044

An attacker with access to the network could be able to install specially crafted firmware to 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:T/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2020-10045

An error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application.

CVSS v3.1 Base Score	8.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:H/E:P/RL:T/RC:C
CWE	CWE-294: Authentication Bypass by Capture-replay

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Luca Simbürger, Luca Hofschuster, Lukas Kahnert, Jakob Lachermeier, Christian Costa, Simon Huber, Lukas Sas Brunschier, Florian Freiberger, Florian Burger, Marie-Louise Oostveen, Magdalena Thomeczek, and Johann Uhrmann from Landshut University of Applied Sciences for coordinated disclosure of CVE-2020-10037
- Max Hirschberger, Simon Hofmann, and Peter Knauer from Augsburg University of Applied Sciences for coordinated disclosure of CVE-2020-10038 to CVE-2020-10045

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 (2020-07-14):	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/