SSA-871704: Multiple Vulnerabilities in SICAM Products

Publication Date: 2024-05-14
Last Update: 2024-06-11
Current Version: V1.1
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 8.6

SUMMARY

Multiple SICAM products are affected by vulnerabilities that could lead to privilege escalation, remote code execution or information loss namely:

- SICAM A8000 device firmwares
  - CPC80 for CP-8000/CP-8021/CP-8022
  - CPCI85 and OPUPI0 for CP-8031/CP-8050
- SICAM EGS firmware
  - CPCI85 and OPUPI0
- SICAM 8 Software Solution
  - SICORE

Siemens has released new versions for the affected firmwares and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
CPC80 Central Processing/Communication: All versions < V16.41 affected by CVE-2024-31484	Update to V16.41 or later version. The firmware CPC80 V16.41 is present within “CP-8000/CP-8021/CP-8022 Package” V16.41 https://support.industry.siemens.com/cs/ww/en/view/109812178/
CPCI85 Central Processing/Communication: All versions < V5.30 affected by CVE-2024-31484, CVE-2024-31485	Update to V5.30 or later version The firmware CPCI85 V5.30 is present within “CP-8031/CP-8050 Package” V5.30 https://support.industry.siemens.com/cs/ww/en/view/109804985/
OPUPI0 AMQP/MQTT: All versions < V5.30 affected by CVE-2024-31486	Update to V5.30 or later version The firmware OPUPI0 V5.30 is present within “CP-8031/CP-8050 Package” V5.30 https://support.industry.siemens.com/cs/ww/en/view/109804985/
SICORE Base system: All versions < V1.3.0 affected by CVE-2024-31485	Update to V1.3.0 or later version The firmware SICORE V1.3.0 is present within “SICAM 8 Software Solution Package” V5.30 https://support.industry.siemens.com/cs/ww/en/view/109818240/

WORKAROUNDS AND MITIGATIONS

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 8 Power automation platform is a universal, hard- and software based, all-in-one solution for all applications in the field of power supply

The SICAM A8000 RTUs (Remote Terminal Units) series is a modular device range for telecontrol and automation applications in all areas of energy supply.

SICAM EGS (Enhanced Grid Sensor) is a gateway for local substations in power distribution grids.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-31484

The affected devices contain an improper null termination vulnerability while parsing a specific HTTP header. This could allow an attacker to execute code in the context of the current process or lead to denial of service condition.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2024-31485

The web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.6
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2024-31486

The affected devices stores MQTT client passwords without sufficient protection on the devices. An attacker with remote shell access or physical access could retrieve the credentials leading to confidentiality loss.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N
CVSS v4.0 Base Score	6.0
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-312: Cleartext Storage of Sensitive Information

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Steffen Robertz, Gerhard Hechenberger, Stefan Viehböck, and Constantin Schieber-Knöbl from SEC Consult Vulnerability Lab for coordinated disclosure of 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 (2024-05-14):	Publication Date
V1.1 (2024-06-11):	Added Constantin Schieber-Knöbl and Stefan Viehböck to the acknowledgment

TERMS OF USE