SSA-185638: Authentication Bypass Vulnerability in SICAM A8000 Web Server Module

Publication Date:	2022-08-09
Last Update:	2022-08-09
Current Version:	V1.0
CVSS v3.1 Base Score:	4.3

SUMMARY

A vulnerability was identified in the web server module used in the SICAM A8000 CP-8000, CP-8021 and CP-8022 devices' protocol firmwares.

- AGPMT0 (AGP Master)
- DNPiT1 (DNP3 TCP/IP Server)
- DNPiT2 (DNP3 TCP/IP Client)
- DNPMT0 (DNP3 Master seriell)
- DNPST0 (DNP3 Slave seriell)
- ET83 (61850 Ed.1)
- ET85 (61850 Ed.2)
- MBCiT0 (MODBUS TCP/IP Client)
- MBSiT0 (MODBUS TCP/IP Server)
- MODMT2 (MODBUS Master seriell)
- OPUPT0 (OPCUA Pub/Sub)
- OPUPT1 (Mindconnect)

The vulnerability could allow unauthenticated access to the web interface of the affected web server module. The module is used for diagnostic purposes as well as commissioning and has to be activated manually within the protocol firmwares. For this reason the protocol firmwares are *secure by default*. Siemens updated the manual to make the situation transparent and raise awareness for operators.

Siemens recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
CP-8000 MASTER MODULE WITH I/O -25/+70°C (6MF2101-0AB10-0AA0): All versions	Currently no fix is planned Operate the affected web server module only when required and consider the security instructions provided in the updated manual (see also Additional Information chapter)
CP-8000 MASTER MODULE WITH I/O -40/+70°C (6MF2101-1AB10-0AA0): All versions	Currently no fix is planned Operate the affected web server module only when required and consider the security instructions provided in the updated manual (see also Additional Information chapter)
CP-8021 MASTER MODULE (6MF2802-1AA00): All versions	Currently no fix is planned Operate the affected web server module only when required and consider the security instructions provided in the updated manual (see also Additional Information chapter)

CP-8022 MASTER MODULE WITH GPRS (6MF2802-2AA00): All versions	Currently no fix is planned Operate the affected web server module only when required and consider the security instructions provided in the updated manual (see also Additional Information chapter)

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

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

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-2021-46304

The component allows to activate a web server module which provides unauthenticated access to its web pages. This could allow an attacker to retrieve debug-level information from the component such as internal network topology or connected systems.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- CybExer Technologies for reporting the vulnerability

ADDITIONAL INFORMATION

The security manual can be downloaded as an individual document from SIOS at: https://support.industry.siemens.com/cs/ww/en/view/109811814

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 (2022-08-09): 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.