SSA-324998: Multiple Vulnerabilities in SICAM A8000

Publication Date: 2022-01-11
Last Update: 2022-01-11
Current Version: V1.0
CVSS v3.1 Base Score: 9.9

SUMMARY

SICAM A8000 devices are impacted by two vulnerabilities. The first one could allow a privileged user to enable a debug port with default credentials. The second vulnerability could allow unauthenticated access to certain previously created log files.

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
CP-8000 MASTER MODULE WITH I/O -25/+70°C (6MF2101-0AB10-0AA0): All versions < V16.20	Update to V16.20 or later version https://support.industry.siemens.com/cs/ww/en/view/109805670
CP-8000 MASTER MODULE WITH I/O -40/+70°C (6MF2101-1AB10-0AA0): All versions < V16.20	Update to V16.20 or later version https://support.industry.siemens.com/cs/ww/en/view/109805670
CP-8021 MASTER MODULE (6MF2802-1AA00): All versions < V16.20	Update to V16.20 or later version https://support.industry.siemens.com/cs/ww/en/view/109805670
CP-8022 MASTER MODULE WITH GPRS (6MF2802-2AA00): All versions < V16.20	Update to V16.20 or later version https://support.industry.siemens.com/cs/ww/en/view/109805670

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

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-2021-45033

An undocumented debug port uses hard-coded default credentials. If this port is enabled by a privileged user, an attacker aware of the credentials could access an administrative debug shell on the affected device.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-798: Use of Hard-coded Credentials

Vulnerability CVE-2021-45034

The web server of the affected system allows access to logfiles and diagnostic data generated by a privileged user. An unauthenticated attacker could access the files by knowing the corresponding download links.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/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:

- Michael Messner 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 (2022-01-11): Publication Date

TERMS OF USE