SSA-669737: Improper Access Control Vulnerability in SICAM TOOLBOX II

Publication Date: 2022-02-08
Last Update: 2022-03-08
Current Version: V1.1
CVSS v3.1 Base Score: 9.9

SUMMARY

SICAM TOOLBOX II contains a vulnerability that could allow an attacker access through a circumventable access control.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM TOOLBOX II: All versions	Currently no remediation is available Restrict port 1522/tcp access to localhost or specific ip addresses only, as documented in the updated security manual (chapter 3.6.7) [1], which is also included in the SICAM TOOLBOX II, V07.01 package [2] [1] https://support.industry.siemens.com/cs/ww/en/view/109757707 [2] https://support.industry.siemens.com/cs/ww/en/view/109805672

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

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 TOOLBOX II is an engineering solution for plants and systems of all sizes. It allows data collection, data modeling, configuration, and parameterization. It is used for engineering of process information for the automation and central control-room systems.

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-2021-45106

Affected applications use a circumventable access control within a database service. This could allow an attacker to access the database.

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:T/RC:C
CWE	CWE-798: Use of Hard-coded Credentials

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Thomas Riedmaier from Siemens Energy for reporting the vulnerability
- Matan Dobrushin and Eran Jacob from OTORIO for reporting the vulnerability

ADDITIONAL INFORMATION

The security manual is included within the SICAM TOOLBOX II package that can be downloaded from SIOS.

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 (2022-02-08): Publication Date
V1.1 (2022-03-08): Updated Acknowledgments; Improved Mitigation Description

TERMS OF USE