SSA-975961: Privilege Escalation Vulnerabilities in SICAM TOOLBOX II before V07.10

Publication Date: 2023-08-08
Last Update: 2023-08-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

SICAM TOOLBOX II contains two vulnerabilities that could allow local attackers to execute code on the system with elevated privileges.

Siemens has released an update for SICAM TOOLBOX II and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM TOOLBOX II: All versions < V07.10	Update to V07.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109822197/ See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Ensure that only trusted persons have access to the system and avoid the configuration of additional local accounts

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 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-2022-39062

Affected applications do not properly set permissions for product folders. This could allow an authenticated attacker with low privileges to replace DLLs and conduct a privilege escalation.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2023-38641

The affected application's database service is executed as `NT AUTHORITY\SYSTEM`. This could allow a local attacker to execute operating system commands with elevated privileges.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-250: Execution with Unnecessary Privileges

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Thomas Riedmaier from Siemens Energy for reporting the vulnerabilities
- Felix Eberstaller and Bernhard Lorenz from Limes Security for reporting the vulnerabilities on behalf of VERBUND Hydro Power GmbH

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 (2023-08-08): Publication Date

TERMS OF USE