SSA-849072: Several Vulnerabilities in SICAM PAS before V8.06

Publication Date: 2022-12-13
Last Update: 2022-12-13
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

SICAM PAS/PQS before V8.06 is affected by three vulnerabilities which could lead to remote code execution, privilege escalation or the creation of a denial of service condition.

Siemens has released several updates for SICAM PAS/PQS and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM PAS/PQS: All versions < V7.0	Update to V7.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109744496/
SICAM PAS/PQS: All versions >= 7.0 < V8.06 only affected by CVE-2022-43723	Update to V8.06 or later version https://support.industry.siemens.com/cs/ww/en/view/109744493/

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

 © Siemens 2022

PRODUCT DESCRIPTION

SICAM PAS/PQS is an energy automation solution for operating an electrical substation with its devices.

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-2022-43722

Affected software does not properly secure a folder containing library files. This could allow an attacker to place a custom malicious DLL in this folder which is then run with SYSTEM rights when a service is started that requires this DLL. At the time of assigning the CVE, the affected firmware version of the component has already been superseded by succeeding mainline versions.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-427: Uncontrolled Search Path Element

Vulnerability CVE-2022-43723

Affected software does not properly validate the input for a certain parameter in the s7ontcp.dll. This could allow an unauthenticated remote attacker to send messages and create a denial of service condition as the application crashes. At the time of assigning the CVE, the affected firmware version of the component has already been superseded by succeeding mainline versions.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-1287: Improper Validation of Specified Type of Input

Vulnerability CVE-2022-43724

Affected software transmits the database credentials for the inbuilt SQL server in cleartext. In combination with the by default enabled xp_cmdshell feature unauthenticated remote attackers could execute custom OS commands. At the time of assigning the CVE, the affected firmware version of the component has already been superseded by succeeding mainline versions.

CVSS v3.1 Base Score	8.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Georgy Zaytsev and Maxim Kozhevnikov from Positive Technologies 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 (2022-12-13): 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.