

## SSA-035466: Incorrect Permission Assignment in SICAM PAS/PQS

Publication Date: 2023-10-10  
Last Update: 2023-10-10  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.8

### SUMMARY

SICAM PAS/PQS is affected by insecure permission assignments in application folders that could allow an authenticated local attacker to read and modify configuration data or to escalate privileges.

Siemens has prepared a security patch and recommends to run it on affected systems to fix the permissions of the impacted folders. This security patch will be integral part of the upcoming SICAM PAS/PQS V8.22 and later versions.

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM PAS/PQS: All versions $\geq$ V8.00 < V8.22 affected by CVE-2023-38640	Install the Security Patch (available at <a href="https://support.industry.siemens.com/cs/ww/en/view/109824392/">https://support.industry.siemens.com/cs/ww/en/view/109824392/</a> ), which can be applied to versions V8.00 to V8.21 Update to V8.22 or later version See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SICAM PAS/PQS: All versions $\geq$ V8.00 < V8.20 affected by CVE-2023-45205	Install the Security Patch (available at <a href="https://support.industry.siemens.com/cs/ww/en/view/109824392/">https://support.industry.siemens.com/cs/ww/en/view/109824392/</a> ), which can be applied to versions V8.00 to V8.21 Update to V8.20 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109815395/">https://support.industry.siemens.com/cs/ww/en/view/109815395/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

### 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 on the server

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 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-2023-38640**

The affected application is installed with specific files and folders with insecure permissions. This could allow an authenticated local attacker to read and modify configuration data in the context of the application process.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

### **Vulnerability CVE-2023-45205**

The affected application is installed with specific files and folders with insecure permissions. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges to **NT AUTHORITY/ SYSTEM**.

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

## **ADDITIONAL INFORMATION**

The Security Patch (<https://support.industry.siemens.com/cs/ww/en/view/109824392/>) is suitable only for use with SICAM PAS/PQS V8.00 to V8.21. It will be integral part of the future releases of SICAM PAS/PQS (V8.22 and later versions).

Note that CVE-2023-45205 is already fixed in V8.20, but can be fixed as well, along with CVE-2023-38640, in earlier versions by applying the Security Patch.

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 (2023-10-10): 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](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.