SSA-145196: Authorization Bypass Vulnerability in Siveillance Control

Publication Date: 2024-03-12
Last Update: 2024-03-12
Current Version: V1.0
CVSS v3.1 Base Score: 5.5
CVSS v4.0 Base Score: 6.8

SUMMARY

Siveillance Control does not properly check the list of access groups that are assigned to an individual user. This could enable a locally logged on user to gain write privileges for objects where they only have read privileges.

Siemens has released a new version for Siveillance Control and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siveillance Control: All versions >= V2.8 < V3.1.1 affected by all CVEs	Update to V3.1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109827073/ See further 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:

- Restrict access to the machine where the Siveillance Control frontend is installed

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

Siveillance Control, formerly known as Siveillance Viewpoint, is a Physical Security Information Management system (PSIM) that seamlessly consolidates a variety of safety and security systems, such as access control, intrusion detection, and video surveillance, all on one common platform.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2023-45793

The affected product does not properly check the list of access groups that are assigned to an individual user. This could enable a locally logged on user to gain write privileges for objects where they only have read privileges.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
CVSS v4.0 Base Score	6.8
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N
CWE	CWE-863: Incorrect Authorization

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 (2024-03-12): 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.