SSA-456933: Multiple Vulnerabilities in SIMATIC PCS neo before V4.1

Publication Date: 2023-11-14
Last Update: 2023-11-14
Current Version: V1.0
CVSS v3.1 Base Score: 8.0

SUMMARY

SIMATIC PCS neo before V4.1 is affected by multiple vulnerabilities.

Siemens has released a new version for SIMATIC PCS neo and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS neo: All versions < V4.1	Update to V4.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109825230/

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

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SIMATIC PCS neo is a distributed control system (DCS).

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-2023-46096

The PUD Manager of affected products does not properly authenticate users in the PUD Manager web service. This could allow an unauthenticated adjacent attacker to generate a privileged token and upload additional documents.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2023-46097

The PUD Manager of affected products does not properly neutralize user provided inputs. This could allow an authenticated adjacent attacker to execute SQL statements in the underlying database.

CVSS v3.1 Base Score	6.3
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2023-46098

When accessing the Information Server from affected products, the products use an overly permissive CORS policy. This could allow an attacker to trick a legitimate user to trigger unwanted behavior.

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-942: Permissive Cross-domain Policy with Untrusted Domains

Vulnerability CVE-2023-46099

There is a stored cross-site scripting vulnerability in the Administration Console of the affected product, that could allow an attacker with high privileges to inject Javascript code into the application that is later executed by another legitimate user.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Michael Messner from Siemens Energy for coordinated disclosure of CVE-2023-46099

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 (2023-11-14): Publication date

TERMS OF USE