SSA-646240: Sensitive Information Disclosure in SIMATIC PCS neo Administration Console

Publication Date: 2023-09-14
Last Update: 2023-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 5.5

SUMMARY

The Administration Console of SIMATIC PCS neo leaks Windows admin credentials. An attacker with local Windows access to the Administration Console could get the credentials, and impersonate the admin user, thereby gaining admin access to other Windows systems.

Siemens has released a security patch for the affected products and recommends to install the patch.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS neo (Administration Console) V4.0: All versions	Install Security Patch 01 https://support.industry.siemens.com/cs/ww/en/view/109824065/ See further recommendations from section Workarounds and Mitigations
SIMATIC PCS neo (Administration Console) V4.0 Update 1: All versions	Install Security Patch 01 https://support.industry.siemens.com/cs/ww/en/view/109824065/ 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:

- Change the password of the Windows accounts used for the remote deployment of AC Agent and avoid to remotely deploy AC Agents

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

 © Siemens 2023

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-2023-38558

The affected application leaks Windows admin credentials. An attacker with local access to the Administration Console could get the credentials, and impersonate the admin user, thereby gaining admin access to other Windows systems.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory

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 (2023-09-14): 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.