SSA-883918: Information Disclosure Vulnerability in SIMATIC WinCC

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 5.9
CVSS v4.0 Base Score: 8.2

SUMMARY

Multiple versions of SIMATIC WinCC and SIMATIC PCS 7 do not properly handle certain requests to their web application (WinCC WebNavigator, PCS 7 Web Serser, and PCS 7 Web Diagnostics Server), which may lead to the leak of privileged information. This could allow an unauthenticated remote attacker to retrieve information such as users and passwords.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS 7 V9.1: All versions affected by CVE-2024-30321	Update WinCC to V7.5 SP2 Update 17 or later version https://support.industry.siemens.com/cs/ww/en/view/109793460/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V18: All versions affected by CVE-2024-30321	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V19: All versions < V19 Update 2 affected by CVE-2024-30321	Update to V19 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109820999/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.4: All versions < V7.4 SP1 Update 23 affected by CVE-2024-30321	Update to V7.4 SP1 Update 23 or later version https://support.industry.siemens.com/cs/ww/en/view/109955792/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.5: All versions < V7.5 SP2 Update 17 affected by CVE-2024-30321	Update to V7.5 SP2 Update 17 or later version https://support.industry.siemens.com/cs/ww/en/view/109793460/ See further recommendations from section Workarounds and Mitigations

SIMATIC WinCC V8.0: All versions < V8.0 Update 5 affected by CVE-2024-30321	Update to V8.0 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109818723/ 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 application webserver for trusted users only

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 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS 7 and other components.

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

SIMATIC WinCC Runtime Professional is a visualization runtime platform used for operator control and monitoring of machines and plants.

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-2024-30321

The affected products do not properly handle certain requests to their web application, which may lead to the leak of privileged information. This could allow an unauthenticated remote attacker to retrieve information such as users and passwords.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v4.0 Base Score	8.2
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-359: Exposure of Private Personal Information to an Unauthorized Actor

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 (2024-07-09):   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.