# SSA-730482: Denial of Service Vulnerability in SIMATIC WinCC

Publication Date:        2024-04-09
Last Update:            2024-07-09
Current Version:        V1.1
CVSS v3.1 Base Score:    6.2
CVSS v4.0 Base Score:    6.9

## SUMMARY

A vulnerability in the login dialog box of SIMATIC WinCC could allow a local attacker to cause a denial of service condition in the runtime of the SCADA system.

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 specific 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:<br>All versions < V9.1 SP2 UC04<br>affected by CVE-2023-50821 | Update to V9.1 SP2 UC04 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109812242/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC Runtime Professional V17:<br>All versions<br>affected by CVE-2023-50821 | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC Runtime Professional V18:<br>All versions < V18 Update 4<br>affected by CVE-2023-50821 | Update to V18 Update 4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109807225/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC Runtime Professional V19:<br>All versions < V19 Update 1<br>affected by CVE-2023-50821 | Update to V19 Update 1 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109820999/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC V7.5:<br>All versions < V7.5 SP2 Update 16<br>affected by CVE-2023-50821 | Update to V7.5 SP2 Update 16 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109793460/<br>See further recommendations from section Workarounds and Mitigations |

| SIMATIC WinCC V8.0:<br><br>All versions < V8.0 Update 5<br>affected by CVE-2023-50821 | Update to V8.0 Update 5 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109818723/<br>See further recommendations from section<br>Workarounds and Mitigations |
|---|---|

## WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Activate SIMATIC Logon in the User Administrator of the SIMATIC PCS 7 Operator Stations

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-2023-50821

The affected products do not properly validate the input provided in the login dialog box. An attacker could leverage this vulnerability to cause a persistent denial of service condition.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.2 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CVSS v4.0 Base Score | 6.9 |
| CVSS Vector | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N |
| CWE | CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') |

## ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Doukani Mohammed Adam from Resilience (resilience.sa) for reporting the vulnerability

## 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 (2024-04-09):    Publication Date
V1.1 (2024-07-09):    Added fix for SIMATIC WinCC V8.0 and SIMATIC WinCC Runtime Professional
                      V18

## 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.