# SSA-753746: Denial of Service Vulnerabilities in SIMATIC WinCC Affecting Other SIMATIC Software Products

Publication Date: 2024-02-13
Last Update: 2024-04-09
Current Version: V1.1
CVSS v3.1 Base Score: 6.5
CVSS v4.0 Base Score: 7.1

## SUMMARY

Two null point dereference vulnerabilities affect multiple SIMATIC software products. These could allow an attacker to cause a persistent denial of service condition in the RPC Server of these products.

Siemens has released new versions for the affected products and recommends to update to the latest versions.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| OpenPCS 7 V9.1:<br>All versions<br>affected by all CVEs | Currently no fix is available<br>The vulnerability is fixed if SIMATIC WinCC V7.5 SP2 Update 15 or later version is installed on the same system<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC BATCH V9.1:<br>All versions<br>affected by all CVEs | Currently no fix is available<br>The vulnerability is fixed if SIMATIC WinCC V7.5 SP2 Update 15 or later version is installed on the same system<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC PCS 7 V9.1:<br>All versions<br>affected by all CVEs | Currently no fix is available<br>Update to V9.1 SP2; then update SIMATIC WinCC to V7.5 SP2 Update 15 or later version<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC Route Control V9.1:<br>All versions<br>affected by all CVEs | Currently no fix is available<br>The vulnerability is fixed if SIMATIC WinCC V7.5 SP2 Update 15 or later version is installed on the same system<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC Runtime Professional V18:<br>All versions<br>affected by all CVEs | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC WinCC Runtime Professional V19:<br>All versions<br>affected by all CVEs | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC V7.4:<br>All versions<br>affected by all CVEs | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC V7.5:<br>All versions < V7.5 SP2 Update 15<br>affected by all CVEs | Update to V7.5 SP2 Update 15 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>All versions < V8.0 SP4<br>affected by all CVEs | Update to V8.0 SP4 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109818723/<br>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:

- Ensure that SIMATIC WinCC, SIMATIC WinCC Runtime Professional and SIMATIC PCS 7 stations communicate via encrypted channels (i.e. activate feature “Encrypted Communication” in SIMATIC WinCC and SIMATIC PCS 7). Enabling “Encrypted Communication” completely mitigates the vulnerability

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-2023-48363

The implementation of the RPC (Remote Procedure call) communication protocol in the affected products do not properly handle certain unorganized RPC messages. An attacker could use this vulnerability to cause a denial of service condition in the RPC server.

| | |
|---|---|
| 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:N/A:H/E:P/RL:O/RC:C |
| CVSS v4.0 Base Score | 7.1 |
| CVSS Vector | CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2023-48364

The implementation of the RPC (Remote Procedure call) communication protocol in the affected products do not properly handle certain malformed RPC messages. An attacker could use this vulnerability to cause a denial of service condition in the RPC server.

| | |
|---|---|
| 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:N/A:H/E:P/RL:O/RC:C |
| CVSS v4.0 Base Score | 7.1 |
| CVSS Vector | CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N |
| CWE | CWE-476: NULL Pointer Dereference |

## ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Yu Cong from EZVIZ for reporting and coordinated disclosure

## 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 (2024-02-13): Publication Date
V1.1 (2024-04-09): Added a mitigation

## TERMS OF USE