SSA-968170: Remote Code Execution Vulnerability in SIMATIC STEP 7 V5.x and Derived Products

Publication Date: 2023-06-13
Last Update: 2024-03-12
Current Version: V1.2
CVSS v3.1 Base Score: 10.0

SUMMARY

SIMATIC STEP 7 and PCS 7 contain a database management system that could allow remote users to use embedded functions of the database (local or in a network share) that have impact on the server.

An attacker with network access to the server network could leverage these embedded functions to run code in the database management system's server (where STEP 7 or PCS 7 are running).

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens 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: All versions < V9.1 SP2 UC04 affected by all CVEs	Update to V9.1 SP2 UC04 or later version https://support.industry.siemens.com/cs/ww/en/view/109812242/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-PM: All versions affected by all CVEs	Currently no fix is planned Switch to “Single terminal system” (as described in the section Workarounds and Mitigations). Alternatively, consider migrating the STEP 7 project to the latest version of TIA Portal and uninstall S7-PM See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 V5: All versions < V5.7 affected by all CVEs	Update to V5.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109794088/ 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:

- If multiple Engineering Systems are in use limit remote access to port 2638/tcp to trusted systems only
- If multiple Engineering Systems are in use ensure that the user accounts in use are restricted to the minimum required operating rights
- If only one Engineering System is in use, consider changing to “Single terminal system” mode in the “Configure SIMATIC Workspace/Workstation” application, under the “Workstation Configuration” tab. Restart the computer. More details can be found in the following FAQ: https://support.industry.siemens.com/cs/ww/en/view/109821340/

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 S7-PM is an option package of SIMATIC STEP 7 V5.7 providing the possibility to use project-wide assignment of message numbers.

SIMATIC STEP 7 V5 is the classic engineering software to configure and program SIMATIC S7-300/S7-400/C7/WinAC controllers.

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-2023-25910

The affected product contains a database management system that could allow remote users with low privileges to use embedded functions of the database (local or in a network share) that have impact on the server.

An attacker with network access to the server network could leverage these embedded functions to run code with elevated privileges in the database management system’s server.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:T/RC:C
CWE	CWE-94: Improper Control of Generation of Code (’Code Injection’)

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Thomas Riedmaier from Siemens Energy 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 (2023-06-13):	Publication Date
V1.1 (2023-07-11):	Added a new mitigations to all affected products, adjusted summary and CVSS score
V1.2 (2024-03-12):	Added fix to SIMATIC PCS 7

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.