SSA-363107: An Improper Initialization Vulnerability Affects SIMATIC WinCC Kiosk Mode

Publication Date: 2022-05-10
Last Update: 2023-11-14
Current Version: V1.4
CVSS v3.1 Base Score: 7.8

SUMMARY

A vulnerability was found in SIMATIC WinCC that could allow authenticated attackers to escape the Kiosk Mode.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS 7 V8.2: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.0: All versions < V9.0 SP3 UC06	Update to V9.0 SP3 UC06 or later version Update SIMATIC WinCC to V7.4 SP 1 Update 21 or later version https://support.industry.siemens.com/cs/ww/en/view/109780528/ See further recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.1: All versions < V9.1 SP1 UC01	Update to V9.1 SP1 UC01 or later version Update SIMATIC WinCC to V7.5 SP2 Update 8 or later version https://support.industry.siemens.com/cs/ww/en/view/109805072/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V16 and earlier: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V17: All versions < V17 Upd4	Update to V17 Upd4 or later version https://support.industry.siemens.com/cs/ww/en/view/109800913/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.3: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC WinCC V7.4: All versions < V7.4 SP1 Update 21	Update to V7.4 SP1 Update 21 or later version https://support.industry.siemens.com/cs/ww/en/view/109806846/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.5: All versions < V7.5 SP2 Update 8	Update to V7.5 SP2 Update 8 or later version https://support.industry.siemens.com/cs/ww/en/view/109793460/ 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:

- At least one default printer (but not a file based printer, as e.g. PDF/XPS printer) should be installed on the affected system
- No file based printer, as e.g. PDF/XPS printers, should be installed on the affected system
- Harden the application's host to prevent local access by untrusted personnel

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 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-2022-24287

A missing printer configuration on the host could allow an authenticated attacker to escape the WinCC Kiosk Mode.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1188: Insecure Default Initialization of Resource

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Tim Dijkman from Powerspex 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 (2022-05-10):	Publication Date
V1.1 (2022-06-14):	Updated fix for SIMATIC PCS 7 V9.1 and added fix for SIMATIC WinCC Runtime Professional V17
V1.2 (2023-07-11):	Added fix for SIMATIC WinCC V7.4 and update remediation for SIMATIC PCS 7 V9.0
V1.3 (2023-10-10):	Added fix for SIMATIC PCS 7 V9.0
V1.4 (2023-11-14):	No fix planned for SIMATIC PCS 7 V8.2

TERMS OF USE