SSA-914168: Multiple Vulnerabilities in SIMATIC WinCC Affecting Other SIMATIC Software Products

Publication Date: 2022-02-08
Last Update: 2022-05-10
Current Version: V1.2
CVSS v3.1 Base Score: 6.3

SUMMARY

Multiple vulnerabilities were found in SIMATIC WinCC that ultimately could allow attackers to retrieve and brute force password hashes and access other systems.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS 7 V8.2: All versions	Install SIMATIC WinCC V7.4 SP1 Update 19 or later version https://support.industry.siemens.com/cs/ww/en/view/109806846/ See further recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.0: All versions	Update to V9.0 SP3 UpdateCollection04 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	Update to V9.1 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109805073/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.4: All versions < V7.4 SP1 Update 19	Update to V7.4 SP1 Update 19 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 6	Update to V7.5 SP2 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109793460/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V15 and earlier: All versions < V15 SP1 Update 7	Update to V15 SP1 Update 7 or later version https://support.industry.siemens.com/cs/us/en/view/109763890/ See further recommendations from section Workarounds and Mitigations

SIMATIC WinCC V16: All versions < V16 Update 5	Update to V16 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109776017/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V17: All versions < V17 Update 2	Update to V17 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109784441/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V17: All versions >= V17 Update 2 only affected by CVE-2021-40363	Currently no fix is available See 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:

- CVE-2021-40363: 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, OpenPCS7 and other components.

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

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-2021-40360

The password hash of a local user account in the remote server could be granted via public API to a user on the affected system. An authenticated attacker could brute force the password hash and use it to login to the server.

CVSS v3.1 Base Score	6.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2021-40363

The affected component stores the credentials of a local system account in a potentially publicly accessible project file using an outdated cipher algorithm. An attacker may use this to brute force the credentials and take over the system.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory

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 (2022-02-08):	Publication Date
V1.1 (2022-04-12):	Added solution for SIMATIC WinCC V7.4, SIMATIC PCS 7 V8.2 and SIMATIC PCS 7 V9.0
V1.2 (2022-05-10):	Added solution for SIMATIC WinCC V15

TERMS OF USE