SSA-840188: Multiple Vulnerabilities in SIMATIC WinCC Affecting Other SIMATIC Software Products

Publication Date: 2021-11-09
Last Update: 2021-11-09
Current Version: V1.0
CVSS v3.1 Base Score: 9.9

SUMMARY

Multiple vulnerabilities were found in SIMATIC WinCC that ultimately could allow local attackers to escalate privileges and read, write or delete critical files.

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 and earlier: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.0: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.1: All versions	Install V7.5 SP2 Update 5 or later version https://support.industry.siemens.com/cs/us/en/view/109793460/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.4 and earlier: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.5: All versions < V7.5 SP2 Update 5	Update to V7.5 SP2 Update 5 or later version https://support.industry.siemens.com/cs/us/en/view/109793460/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V15 and earlier: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC V16: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC V17: All versions	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:

- Harden the application's host to prevent local access by untrusted personnel

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-2021-40358

Legitimate file operations of the affected systems do not properly neutralize special elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read, write or delete unexpected critical files.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2021-40359

When downloading files, the affected systems do not properly neutralize special elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read unexpected critical files.

CVSS v3.1 Base Score	7.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2021-40364

The affected systems store sensitive information in log files. An attacker with access to the log files could publicly expose the information or reuse it to develop further attacks on 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-532: Insertion of Sensitive Information into Log File

ACKNOWLEDGMENTS

Siemens thanks the following parties for their 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 (2021-11-09): Publication Date

TERMS OF USE