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

Publication Date: 2021-11-09
Last Update: 2023-04-11
Current Version: V1.6
CVSS v3.1 Base Score: 9.9

SUMMARY

Multiple vulnerabilities were found in SIMATIC WinCC that ultimately could allow local or remote 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 recommends specific countermeasures for products where updates are not, or not yet available.

Note: The vulnerability CVE-2021-40359 is part of a shared component, used by various Siemens products (SIMATIC Communication Services - SCS). The installation of a fix version of any product also removes the vulnerability for other products on the same system, even if those products were not updated.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
OpenPCS 7 V8.2: All versions only affected by CVE-2021-40359	Currently no fix is planned The vulnerability is fixed if SIMATIC WinCC V7.4 SP1 Update 19 or later version is installed on the same system See further recommendations from section Workarounds and Mitigations
OpenPCS 7 V9.0: All versions < V9.0 Upd4 only affected by CVE-2021-40359	Update to V9.0 Upd4 or later version; V9.0 Upd4 is bundled in PCS 7 V9.0 SP3 UC04 https://support.industry.siemens.com/cs/ww/en/view/109780528/ See further recommendations from section Workarounds and Mitigations
OpenPCS 7 V9.1: All versions only affected by CVE-2021-40359	See remediation for SIMATIC PCS 7 V9.1 See further recommendations from section Workarounds and Mitigations
SIMATIC BATCH V8.2: All versions only affected by CVE-2021-40359	Currently no fix is planned The vulnerability is fixed if SIMATIC WinCC V7.4 SP1 Update 19 or later version is installed on the same system See further recommendations from section Workarounds and Mitigations
SIMATIC BATCH V9.0: All versions only affected by CVE-2021-40359	Currently no fix is planned The vulnerability is fixed if SIMATIC WinCC V7.4 SP1 Update 19 or later version is installed on the same system See further recommendations from section Workarounds and Mitigations

SIMATIC BATCH V9.1: All versions only affected by CVE-2021-40359	See remediation for SIMATIC PCS 7 V9.1 See further recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V14: All versions only affected by CVE-2021-40359	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V15: All versions only affected by CVE-2021-40359	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V16: All versions < V16 Update 6 only affected by CVE-2021-40359	Update to V16 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811815/ See further recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V17: All versions < V17 SP1 only affected by CVE-2021-40359	Update to V17 SP1 or later version https://support.industry.siemens.com/cs/ww/de/view/109808270/ See further recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V8.2: All versions	Update to V8.2 SP1; then update SIMATIC WinCC to V7.4 SP1 Update 19 or later version to fix CVE-2021-40358 and CVE-2021-40364 https://support.industry.siemens.com/cs/ww/en/view/109806846/ To fix CVE-2021-40359 see chapter “Additional Information” See further recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.0: All versions < V9.0 SP3 UC04	Update to V9.0 SP3 UC04 or later version to fix CVE-2021-40358 and CVE-2021-40364 https://support.industry.siemens.com/cs/ww/en/view/109780528/ To fix CVE-2021-40359 see chapter “Additional Information” 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 Route Control V8.2: All versions only affected by CVE-2021-40359	Currently no fix is planned The vulnerability is fixed if SIMATIC WinCC V7.4 SP1 Update 19 or later version is installed on the same system See further recommendations from section Workarounds and Mitigations

SIMATIC Route Control V9.0: All versions only affected by CVE-2021-40359	Currently no fix is planned The vulnerability is fixed if SIMATIC WinCC V7.4 SP1 Update 19 or later version is installed on the same system See further recommendations from section Workarounds and Mitigations
SIMATIC Route Control V9.1: All versions only affected by CVE-2021-40359	See remediation for SIMATIC PCS 7 V9.1 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 5	Update to V7.5 SP2 Update 5 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

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- CVE-2021-40364: Harden the application's host to prevent local access by untrusted personnel
- CVE-2021-40358: Disable the webserver or only enable it temporarily, when needed

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 NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

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.

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 on the web server 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 party for its efforts:

- Thomas Riedmaier from Siemens Energy for reporting the vulnerabilities CVE-2021-40358 and CVE-2021-40359

ADDITIONAL INFORMATION

The vulnerability CVE-2021-40359 is part of a shared component, used by various Siemens products (SIMATIC Communication Services - SCS). The installation of a fix version of any product also removes the vulnerability for other products on the same system, even if those products were not updated.

SIMATIC PCS 7 V8.2 SP1 supports the update to the following component that fixes CVE-2021-40359: WinCC V7.4 SP1 Update 19.

SIMATIC PCS 7 V9.0 SP3 UC04 contains the following components that fix CVE-2021-40359: OpenPCS 7 V9.0 Upd4 and WinCC V7.4 SP1 Update 19.

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
V1.1 (2022-02-08):	Added solution for SIMATIC WinCC V16 and V17 and adjusted solution for SIMATIC PCS 7 V9.1
V1.2 (2022-03-08):	Added Mitigation to CVE-2021-40358
V1.3 (2022-04-12):	Added solution for SIMATIC WinCC V7.4; added solution for SIMATIC PCS 7 V8.2 and SIMATIC PCS 7 V9.0 and related components; added SIMATIC NET PC Software incl. solution for V17; added a note regarding shared components
V1.4 (2022-05-10):	Added solution for SIMATIC WinCC V15
V1.5 (2022-07-12):	Added fix for SIMATIC NET PC Software V16
V1.6 (2023-04-11):	No fix planned for OpenPCS 7 V8.2, for SIMATIC BATCH V8.2 and V9.0 and for SIMATIC Route Control V8.2 and V9.0

TERMS OF USE