SSA-944678: Potential Password Protection Bypass in SIMATIC WinCC

Publication Date: 2021-02-09
Last Update: 2021-02-09
Current Version: V1.0
CVSS v3.1 Base Score: 6.2

SUMMARY

A vulnerability in the SIMATIC WinCC Graphics Designer tool could allow an attacker that has physical access to a machine running the software to get access to the user's private password-protected pictures.

Siemens has released an update for SIMATIC WinCC and recommends to update to the latest version. Siemens recommends specific countermeasures for PCS 7 as the affected feature is not officially supported.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS 7: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC: All versions < V7.5 SP2	Update to V7.5 SP2 or later version https://support.industry.siemens.com/cs/ww/en/view/109783853/

WORKAROUNDS AND MITIGATIONS

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

- Tailor user privileges to each user's specific needs (need-to-know principle)
- Limit access to the affected products by implementing strict access control mechanisms
- Specific for PCS 7:
  - The affected WinCC-feature is not officially supported and not used by PCS 7. We recommend not to use it and apply the measures described in SIMATIC PCS 7 Compendium Part F.

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

SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS7 and other components.

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-2020-10048

Due to an insecure password verification process, an attacker could bypass the password protection set on protected files, thus being granted access to the protected content, circumventing authentication.

CVSS v3.1 Base Score	6.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-288: Authentication Bypass Using an Alternate Path or Channel

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Enrique Murias Fernandez from Tecdesoft Automation 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 (2021-02-09): Publication Date

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.