SSA-931064: Authentication Bypass in SIMATIC Logon

Publication Date: 2017-02-13
Last Update: 2018-06-12
Current Version: V1.4
CVSS v3.0 Base Score: 9.0

SUMMARY

The latest update for SIMATIC Logon fixes a security vulnerability that could allow attackers to circumvent user authentication under certain conditions.

SIMATIC WinCC, SIMATIC PCS 7, SIMATIC PDM, and SIMATIC IT Production Suite provide SIMATIC Logon as component of the product. Installing the SIMATIC Logon update fixes the vulnerability for all products mentioned below.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Logon: All versions < V1.5 SP3 Update 2	Update to V1.5 SP3 Update 2 https://support.industry.siemens.com/cs/ww/en/view/109744966
SIMATIC WinCC: All versions < V7.4 SP1	Install SIMATIC Logon update (can be installed without WinCC update, see compatibility note on download page) https://support.industry.siemens.com/cs/ww/en/view/109744966
SIMATIC WinCC Runtime Professional: All versions < V14 SP1	Install SIMATIC Logon update (can be installed without WinCC Runtime Professional update, see compatibility note on download page) https://support.industry.siemens.com/cs/ww/en/view/109744966
SIMATIC PCS 7: All versions < V8.2 SP1	Install SIMATIC Logon update (can be installed without PCS 7 update, see compatibility note on download page) https://support.industry.siemens.com/cs/ww/en/view/109744966
SIMATIC PDM: All versions < V9.1	Install SIMATIC Logon update (can be installed without PDM update, see compatibility note on download page) https://support.industry.siemens.com/cs/ww/en/view/109744966
SIMATIC IT Production Suite: All versions < V7.1	Install SIMATIC Logon update (can be installed without IT Production Suite update, see compatibility note on download page) https://support.industry.siemens.com/cs/ww/en/view/109744966

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

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 Logon (SL) is a software application used for central user administration and access control in other SIMATIC applications.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2017-2684

An attacker with knowledge of a valid user name, and physical or network access to the affected system could bypass the application-level authentication.

CVSS v3.0 Base Score	9.0
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C

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 (2017-02-13):	Publication Date
V1.1 (2017-06-13):	Added version information of WinCC 7.4 SP1, WinCC Professional V14 SP1 that include a fixed version of SIMATIC Logon
V1.2 (2017-07-06):	Added version information SIMATIC PCS 7 and SIMATIC PDM that include a fixed version of SIMATIC Logon
V1.3 (2017-11-17):	Added version information for SIMATIC IT Production Suite
V1.4 (2018-06-12):	New format, updated fixed PCS 7 version

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.