SSA-233109: Web Vulnerabilities in SIMATIC Panels

Publication Date: 2018-11-13
Last Update: 2020-02-10
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

The latest update for SIMATIC Panel software and SIMATIC WinCC (TIA Portal) fixes two web vulnerabilities. The most severe is a vulnerability which could allow an attacker with network access to the integrated webserver to download arbitrary files.

Siemens recommends to update to the newest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants): All versions < V15 Update 4	Update SIMATIC WinCC (TIA Portal) to V15 Update 4 or newer, and then update panel to V15 Update 4 or newer. https://support.industry.siemens.com/cs/ww/en/view/109755826
SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants): All versions < V15 Update 4	Update SIMATIC WinCC (TIA Portal) to V15 Update 4 or newer, and then update panel to V15 Update 4 or newer. https://support.industry.siemens.com/cs/ww/en/view/109755826
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F: All versions < V15 Update 4	Update SIMATIC WinCC (TIA Portal) to V15 Update 4 or newer, and then update panel to V15 Update 4 or newer. https://support.industry.siemens.com/cs/ww/en/view/109755826
SIMATIC WinCC Runtime Advanced: All versions < V15 Update 4	Update to V15 Update 4 or newer https://support.industry.siemens.com/cs/ww/en/view/109755826
SIMATIC WinCC Runtime Professional: All versions < V15 Update 4	Update to V15 Update 4 or newer https://support.industry.siemens.com/cs/ww/en/view/109755826
SIMATIC WinCC (TIA Portal): All versions < V15 Update 4	Update to V15 Update 4 or newer https://support.industry.siemens.com/cs/ww/en/view/109755826
SIMATIC HMI Classic Devices - TP/MP/OP/MP Mobile Panel (incl. SIPLUS variants): 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:

- Restrict network access to the integrated web server.
- Deactivate the web server if not required. The web server is disabled by default.

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 Runtime Advanced is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC WinCC Runtime Professional is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

SIMATIC WinCC (TIA Portal) is an engineering software to configure and program SIMATIC Panels, SIMATIC Industrial PCs, and Standard PCs running WinCC Runtime Advanced or SCADA System WinCC Runtime Professional visualization software.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2018-13812

A directory traversal vulnerability could allow to download arbitrary files from the device.

The security vulnerability could be exploited by an attacker with network access to the integrated web server. No user interaction and no authenitcation is required to exploit the vulnerability. The vulnerability impacts the confidentiality of the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/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-2018-13813

The webserver of affected HMI devices may allow URL redirections to untrusted websites.

An attacker must trick a valid user who is authenticated to the device into clicking on a malicious link to exploit the vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-601: URL Redirection to Untrusted Site (‘Open Redirect’)

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Hosni Tounsi from Carthage Red Team // Carthage Cyber Services for coordinated disclosure of CVE-2018-13812
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2018-11-13):	Publication Date
V1.1 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

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.