SSA-804486: Multiple Vulnerabilities in SIMATIC Panels and SIMATIC WinCC (TIA Portal)

Publication Date: 2019-05-14
Last Update: 2019-05-14
Current Version: V1.0
CVSS v3.0 Base Score: 6.5

SUMMARY

The latest update for SIMATIC Panel Software and SIMATIC WinCC (TIA Portal) fixes two vulnerabilities. The most severe is a vulnerability which could allow an attacker with network access to the integrated device to read and write variables via SNMP.

Siemens recommends to update to the newest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC HMI Comfort Panels 4" - 22": All versions < V15.1 Update 1	Update SIMATIC WinCC (TIA Portal) to V15.1 Update 1 or newer, and then update panel to V15.1 Update 1 or newer. https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC HMI Comfort Outdoor Panels 7" & 15": All versions < V15.1 Update 1	Update SIMATIC WinCC (TIA Portal) to V15.1 Update 1 or newer, and then update panel to V15.1 Update 1 or newer. https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 und KTP900F: All versions < V15.1 Update 1	Update SIMATIC WinCC (TIA Portal) to V15.1 Update 1 or newer, and then update panel to V15.1 Update 1 or newer. https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC WinCC Runtime Advanced: All versions < V15.1 Update 1	Update to V15.1 Update 1 or newer https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC WinCC Runtime Professional: All versions < V15.1 Update 1	Update to V15.1 Update 1 or newer https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC WinCC (TIA Portal): All versions < V15.1 Update 1	Update to V15.1 Update 1 or newer https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC HMI Classic Devices (TP/MP/OP/MP Mobile Panel): 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 access to the web interface of the affected devices
- Restrict access to port 161/udp to trusted devices

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), 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.

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-2019-6572

The affected device offered SNMP read and write capacities with a publicly know hardcoded community string.

The security vulnerability could be exploited by an attacker with network access to the affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality and integrity of the affected system.

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

CVSS v3.0 Base Score	6.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2019-6576

An attacker with network access to affected devices could potentially obtain a TLS session key. If the attacker is able to observe TLS traffic between a legitimate user and the device, then the attacker could decrypt the TLS traffic.

The security vulnerability could be exploited by an attacker who has network access to the web interface of the device and who is able to observe TLS traffic between legitimate users and the web interface of the affected device. The vulnerability could impact the confidentiality of the communication between the affected device and a legitimate user.

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

CVSS v3.0 Base Score	5.9
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C

Vulnerability CVE-2019-6577

The integrated web server could allow Cross-Site Scripting (XSS) attacks if an attacker is able to modify particular parts of the device configuration via SNMP.

The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires system privileges and user interaction. An attacker could use the vulnerability to compromise confidentiality and the integrity of the affected system.

At the stage of publishing this security advisory no public exploitation is known.

CVSS v3.0 Base Score	5.4
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N/E:P/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 (2019-05-14): 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.

