SSA-487246: Vulnerabilities in SIMATIC HMI Devices

Publication Date: 2015-04-08
Last Update: 2020-02-10
Current Version: V1.3
CVSS v3.1 Base Score: 8.1

SUMMARY

The latest updates for the affected products fix three vulnerabilities. The most severe of these vulnerabilities could allow an attacker to perform a Denial-of-Service attack against HMI panels under certain conditions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Automation Tool: All versions < V1.0.2	Update to V1.0.2 https://support.industry.siemens.com/cs/ww/en/view/98161300
SIMATIC HMI Basic Panels 1st Generation (WinCC TIA Portal) V12 (incl. SIPLUS variants): All versions < WinCC (TIA Portal) V12 SP1 Upd5	Update to WinCC (TIA Portal) V12 SP1 Upd5 https://support.industry.siemens.com/cs/ww/en/view/78683919
SIMATIC HMI Basic Panels 1st Generation (WinCC TIA Portal) V13 (incl. SIPLUS variants): All versions < WinCC (TIA Portal) V13 SP1 Upd4	Update to WinCC (TIA Portal) V13 SP1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109311724
SIMATIC HMI Basic Panels 2nd Generation V13 (incl. SIPLUS variants): All versions < WinCC (TIA Portal) V13 SP1 Upd2	Update to WinCC (TIA Portal) V13 SP1 Upd2 https://support.industry.siemens.com/cs/ww/en/view/109311724
SIMATIC HMI Comfort Panels V12 (incl. SIPLUS variants): All versions < WinCC (TIA Portal) V12 SP1 Upd5	Update to WinCC (TIA Portal) V12 SP1 Upd5 https://support.industry.siemens.com/cs/ww/en/view/78683919
SIMATIC HMI Comfort Panels V13 (incl. SIPLUS variants): All versions < WinCC (TIA Portal) V13 SP1 Upd2	Update to WinCC (TIA Portal) V13 SP1 Upd2 https://support.industry.siemens.com/cs/ww/en/view/109311724
SIMATIC HMI Mobile Panel 277 (WinCC TIA Portal) V12: All versions < WinCC (TIA Portal) V12 SP1 Upd5	Update to WinCC (TIA Portal) V12 SP1 Upd5 https://support.industry.siemens.com/cs/ww/en/view/78683919

SIMATIC HMI Mobile Panel 277 (WinCC TIA Portal) V13: All versions < WinCC (TIA Portal) V13 SP1 Upd4	Update to WinCC (TIA Portal) V13 SP1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109311724
SIMATIC HMI Multi Panels (WinCC TIA Portal) V12 (incl. SIPLUS variants): All versions < WinCC (TIA Portal) V12 SP1 Upd5	Update to WinCC (TIA Portal) V12 SP1 Upd5 https://support.industry.siemens.com/cs/ww/en/view/78683919
SIMATIC HMI Multi Panels (WinCC TIA Portal) V13 (incl. SIPLUS variants): All versions < WinCC (TIA Portal) V13 SP1 Upd4	Update to WinCC (TIA Portal) V13 SP1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109311724
SIMATIC NET PC-Software V12: All versions < V12 SP2 HF3	Update to V12 SP2 HF3 https://support.industry.siemens.com/cs/ww/en/view/109475388
SIMATIC NET PC-Software V13: All versions < V13 HF1	Update to V13 HF1 https://support.industry.siemens.com/cs/ww/en/view/109475388
SIMATIC WinCC < V7.3: All versions < V7.2 Upd11	Update to V7.2 Upd11 https://support.industry.siemens.com/cs/de/en/view/109478834
SIMATIC WinCC Runtime Advanced V12: All versions < WinCC Runtime Advanced V12 SP1 Upd5	Update to WinCC Runtime Advanced V12 SP1 Upd5 https://support.industry.siemens.com/cs/ww/en/view/79684570
SIMATIC WinCC Runtime Advanced V13: All versions < WinCC Runtime Advanced V13 SP1 Upd2	Update to WinCC Runtime Advanced V13 SP1 Upd2 https://support.industry.siemens.com/cs/ww/en/view/109311423
SIMATIC WinCC Runtime Professional V13: All versions < WinCC (TIA Portal) V13 SP1 Upd2	Update to WinCC (TIA Portal) V13 SP1 Upd2 https://support.industry.siemens.com/cs/ww/en/view/109439573
SIMATIC WinCC V7.3: All versions < V7.3 Upd4	Update to V7.3 Upd4 https://support.industry.siemens.com/cs/de/en/view/109475497

WORKAROUNDS AND MITIGATIONS

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

- Apply cell protection concept (see https://www.siemens.com/cert/operational-guidelines-industrial-security)
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth (see http://www.industry.siemens.com/topics/global/en/industrial-security/concept/Pages/defense-in-depth.aspx)

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 HMI Panels, SIMATIC WinCC Runtime Advanced, and SIMATIC WinCC Runtime Professional are used for operator control and monitoring of machines and plants.

SIMATIC NET PC-Software is required for communication between controller (SIMATIC S7 controller) and PC based solutions (e.g. SIMATIC WinCC).

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system. It is used to monitor and control physical processes involved in industry and infrastructure on a large scale and over long distances.

SIMATIC Automation Tool allows commissioning, adjusting and service in combination with S7-1200 and S7-1500 Controllers without engineering framework.

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-2015-1601

Attackers with access to the network path between PLCs and their communication partners could possibly intercept or modify Siemens industrial communications at port 102/tcp and conduct a Man-in-the-Middle attack. This vulnerability affects all listed products.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-310: Cryptographic Issues

Vulnerability CVE-2015-2822

Attackers with access to the network path between an HMI panel and a PLC (Man-in-theMiddle) could possibly conduct a Denial-of-Service attack against the HMI panel by sending specially crafted packets to the HMI (port 102/tcp). This vulnerability affects SIMATIC WinCC Comfort Panels and SIMATIC WinCC Runtime Advanced.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-310: Cryptographic Issues

Vulnerability CVE-2015-2823

If attackers obtain password hashes for SIMATIC WinCC users, they could possibly use the hashes to authenticate themselves. This vulnerability affects SIMATIC WinCC.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-836: Use of Password Hash Instead of Password for Authentication

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Quarkslab team for coordinated disclosure of CVE-2015-1601 and CVE-2015-2822
- Ilya Karpov from Positive Technologies for coordinated disclosure of CVE-2015-2823
- 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 (2015-04-08):	Publication Date
V1.1 (2015-07-21):	Added update information for SIMATIC HMI Basic Panels 1st Generation (WinCC TIA Portal), SIMATIC HMI Mobile Panel 277 (WinCC TIA Portal), and SIMATIC HMI Multi Panels (WinCC TIA Portal)
V1.2 (2015-08-27):	Added updates for TIA V12 SP1 devices and WinCC V7.2
V1.3 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE

additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.