SSA-487246: Vulnerabilities in SIMATIC HMI Devices

Publication Date 2015-04-08
Last Update 2015-08-27
Current Version 1.2
CVSS Overall Score 5.6

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

- SIMATIC HMI Basic Panels 2nd Generation:
  - V13: All versions < WinCC (TIA Portal) V13 SP1 Upd2
- SIMATIC HMI Comfort Panels:
  - V12: All versions < WinCC (TIA Portal) V12 SP1 Upd5
  - V13: All versions < WinCC (TIA Portal) V13 SP1 Upd2
- SIMATIC WinCC Runtime Advanced:
  - V12: All versions < WinCC Runtime Advanced V12 SP1 Upd5
  - V13: All versions < WinCC Runtime Advanced V13 SP1 Upd2
- SIMATIC WinCC Runtime Professional:
  - V13: All versions < WinCC (TIA Portal) V13 SP1 Upd2
- SIMATIC HMI Basic Panels 1st Generation (WinCC TIA Portal):
  - V12: All versions < WinCC (TIA Portal) V12 SP1 Upd5
  - V13: All versions < WinCC (TIA Portal) V13 SP1 Upd4
- SIMATIC HMI Mobile Panel 277 (WinCC TIA Portal):
  - V12: All versions < WinCC (TIA Portal) V12 SP1 Upd5
  - V13: All versions < WinCC (TIA Portal) V13 SP1 Upd4
- SIMATIC HMI Multi Panels (WinCC TIA Portal):
  - V12: All versions < WinCC (TIA Portal) V12 SP1 Upd5
  - V13: All versions < WinCC (TIA Portal) V13 SP1 Upd4
- SIMATIC NET PC-Software V12 and V13:
  - SIMATIC NET PC-Software V12: All versions < V12 SP2 HF3
  - SIMATIC NET PC-Software V13: All versions < V13 HF1
- SIMATIC WinCC V7.X:
  - All versions prior to V7.2
  - V7.2: All version < V7.2 Upd11
  - V7.3: All versions < V7.3 Upd4
- SIMATIC Automation Tool: All versions < V1.0.2

 © Siemens AG 2015

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.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://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 1 (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 Base Score	5.8
CVSS Temporal Score	4.5
CVSS Overall Score	4.5 (AV:N/AC:M/Au:N/C:P/I:P/A:N/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2015-2822)

Attackers with access to the network path between an HMI panel and a PLC (Man-in-the-Middle) 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 Base Score	7.1
CVSS Temporal Score	5.6
CVSS Overall Score	5.6 (AV:N/AC:M/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C)

Vulnerability 3 (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 Base Score	6.8
CVSS Temporal Score	5.3
CVSS Overall Score	5.3 (AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Mitigating factors

For vulnerability 1 and 2, the attacker must have access to the network path between communication parties.

For vulnerability 3, the attacker must obtain a password hash.

Siemens recommends operating the affected products only within trusted networks [10].

SOLUTION

Siemens provides updates for the following products and recommends customers to update to the new fixed versions:

- SIMATIC HMI Basic Panels 2nd Generation:
  - V13: Update to WinCC (TIA Portal) V13 SP1 Upd2 [1]
- SIMATIC HMI Comfort Panels:
  - V12: Update to WinCC (TIA Portal) V12 SP1 Upd5 [7]
  - V13: Update to WinCC (TIA Portal) V13 SP1 Upd2 [1]
- SIMATIC WinCC Runtime Advanced:
  - V12: Update to V12 SP1 Upd5 [8]
  - V13: Update to V13 SP1 Upd2 [2]
- SIMATIC WinCC Runtime Professional:
  - V13: Update to V13 SP1 Upd2 [3]
- SIMATIC HMI Basic Panels 1st Generation (WinCC TIA Portal):
  - V12: Update to WinCC (TIA Portal) V12 SP1 Upd5 [7]
  - V13: Update to WinCC (TIA Portal) V13 SP1 Upd4 [1]
- SIMATIC HMI Mobile Panel 277 (WinCC TIA Portal):
  - V12: Update to WinCC (TIA Portal) V12 SP1 Upd5 [7]
  - V13: Update to WinCC (TIA Portal) V13 SP1 Upd4 [1]
- SIMATIC HMI Multi Panels (WinCC TIA Portal):
  - V12: Update to WinCC (TIA Portal) V12 SP1 Upd5 [7]
  - V13: Update to WinCC (TIA Portal) V13 SP1 Upd4 [1]
- SIMATIC NET PC-Software V12 and V13:
  - SIMATIC NET PC-Software V12: Update to V12 SP2 HF3 [4]
  - SIMATIC NET PC-Software V13: Update to V13 HF1 [4]
- SIMATIC WinCC V7.X:
  - V7.2 and all versions prior to V7.2: Update to V7.2 Upd11 [9]
  - V7.3: Update to V7.3 Upd4 [5]
- SIMATIC Automation Tool: Update to V1.0.2 [6]

Until patches can be applied, Siemens recommends customers to mitigate the risk of their products by implementing the following steps:

- Apply cell protection concept [10]
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth [11]

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [10] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Quarkslab team for coordinated disclosure of vulnerability 1 and 2.
- Ilya Karpov from Positive Technologies for coordinated disclosure of vulnerability 3.

ADDITIONAL RESOURCES

[1] Update 4 and Update 2 for SIMATIC WinCC (TIA Portal) V13 SP1 can be obtained here:
https://support.industry.siemens.com/cs/ww/en/view/109311724

[2] Update 2 for SIMATIC WinCC Runtime Advanced V13 SP1 can be obtained here:
https://support.industry.siemens.com/cs/ww/en/view/109311423

[3] Update 2 for SIMATIC WinCC Runtime Professional V13 SP1 can be obtained here:
https://support.industry.siemens.com/cs/ww/en/view/109439573

[4] Updates for SIMATIC NET PC-Software can be obtained here:
https://support.industry.siemens.com/cs/ww/en/view/109475388

[5] Update 4 for SIMATIC WinCC V7.3 can be obtained here:
https://support.industry.siemens.com/cs/de/en/view/109475497

[6] Update 2 for SIMATIC Automation Tool can be obtained here:
https://support.industry.siemens.com/cs/ww/en/view/98161300

[7] Update 5 for SIMATIC WinCC (TIA Portal) V12 SP1 can be obtained here:
https://support.industry.siemens.com/cs/ww/en/view/78683919

[8] Update 5 for SIMATIC WinCC Runtime Advanced V12 SP1 can be obtained here:
https://support.industry.siemens.com/cs/ww/en/view/79684570

[9] Update 11 for SIMATIC WinCC V7.2 can be obtained here:
https://support.industry.siemens.com/cs/de/en/view/109478834

[10] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[11] Further information about Defense-in-Depth:
http://www.industry.siemens.com/topics/global/en/industrial-security/concept/Pages/defense-in-depth.aspx

[12] Information about Industrial Security by Siemens:
http://www.siemens.com/industrialsecurity

[13] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
http://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

DISCLAIMER

See: http://www.siemens.com/terms_of_use