SSA-543623: Vulnerabilities in SIMATIC WinCC (TIA Portal) V13

Publication Date	2015-02-13
Last Update	2015-02-13
Current Version	V1.0
CVSS Overall Score	5.3

Summary:

The latest update for SIMATIC WinCC (TIA Portal) V13 fixes two vulnerabilities. One of the vulnerabilities could allow privilege escalation regarding WinCC RT Professional under certain conditions. The attacker must have network access to the WinCC RT Professional application to exploit the vulnerability.

All vulnerabilities resolved with this software release are discussed below.

AFFECTED PRODUCTS

- SIMATIC WinCC (TIA Portal): All versions < V13 SP1

DESCRIPTION

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.

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-2015-1358)

The remote management module of WinCC (TIA Portal) Multi Panels and Comfort Panels, and WinCC RT Advanced transmits weakly protected credentials over the network. Attackers capturing network traffic of the remote management module could possibly reconstruct used passwords.

CVSS Base Score	4.3
CVSS Temporal Score	4.3
CVSS Overall Score	3.4 (AV:N/AC:M/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2014-4686)

A hard coded encryption key used in WinCC RT Professional could allow attackers to escalate their privileges if the application’s network communication with an authenticated user was captured.

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

Vulnerability 1 can only be exploited if the attacker could set up an attack from a privileged network position that allows capturing network traffic of the remote management module.

For vulnerability 2, network access to the corresponding port is required.

Siemens recommends operating SIMATIC WinCC (TIA Portal) Panels and Runtime Systems only within trusted networks [2].

SOLUTION

Siemens provides Service Pack 1 for SIMATIC WinCC (TIA Portal) V13 [1] which fixes the vulnerabilities.

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 [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks Gleb Gritsai, Roman Ilin, Aleksandr Tlyapov, and Sergey Gordeychik from Positive Technologies for coordinated disclosure.

ADDITIONAL RESOURCES

[1] The software update for WinCC (TIA Portal) can be obtained here:
http://support.automation.siemens.com/WW/view/en/106567433

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf

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

[4] 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 (2015-02-13): Publication Date

DISCLAIMER