SSA-064884: Vulnerabilities in WinCC (TIA Portal)

Publication Date 2013-07-31
Last Update 2013-07-31
Current Version V1.1
CVSS Overall Score 4.5

Summary:

Siemens was notified that SIMATIC HMI panels configured by WinCC (TIA Portal) V11 and V12 may contain vulnerabilities. The vulnerabilities affect the web server of the engineered HMIs, and may allow CSRF and open redirect attacks.

Siemens provides a software update that fixes the vulnerabilities.

AFFECTED PRODUCTS

SIMATIC HMI devices managed with the following software:

- WinCC (TIA Portal) V11: all versions
- WinCC (TIA Portal) V12: all versions < V12 SP1

DESCRIPTION

WinCC (TIA Portal) is engineering software for configuring SIMATIC Panels, SIMATIC Industrial PCs, and Standard PCs. with the WinCC Runtime Advanced or the SCADA System WinCC Runtime Professional visualization software.

When configuring a SIMATIC HMI panel with WinCC (TIA Portal), a web server may be activated on the affected devices. This web server may allow attacks based on CSRF (Cross-site request forgery) and URL redirection to untrusted websites.

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-2013-4911)

The web server of the affected HMI panels may allow CSRF (Cross-site request forgery) attacks, compromising integrity and availability of the system.

CVSS Base Score 5.8
CVSS Temporal Score 4.5
CVSS Overall Score 4.5 (AV:N/AC:M/Au:N/C:N/I:P/A:P/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2013-4912)

The web server of the affected HMI panels may allow URL redirection to untrusted websites.

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

Mitigating factors:

The attacker must trick authenticated users of the devices to open malicious web pages. Siemens recommends operating the devices only within trusted networks [3].

SOLUTION

Siemens provides software update WinCC (TIA Portal) V12 SP1 which fixes both vulnerabilities [1]. WinCC (TIA Portal) V11 users should also upgrade to this software version. After installing the software update, upgrade the device firmware by using the function "Change Device/Version" in the user interface. As a further mitigation measure, Siemens strongly recommends to protect the network access to the Web Navigator web interface with appropriate mechanisms.

In general, Siemens strongly recommends to protect systems according to recommended security practices [4] and to configure the environment according to operational guidelines [2] in order to run the affected software components in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Timur Yunusov and Sergey Bobrov from Positive Technologies for coordinated disclosure.

ADDITIONAL RESOURCES

1. The software update may be downloaded via the customer support portal: http://support.automation.siemens.com/WW/view/en/73947391
2. An overview of the operational guidelines for Industrial Security (with the cell protection concept): http://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. Recommended security practices by ICS-CERT: http://ics-cert.us-cert.gov/content/recommended-practices
5. 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 (2013-07-31): Publication date
V1.1 (2013-07-31): Updated advisory title

DISCLAIMER