SSA-315836: Vulnerabilities in SIMATIC STEP 7 (TIA Portal) V12 and V13

Publication Date 2015-02-17
Last Update 2015-08-27
Current Version V1.1
CVSS Overall Score 4.5

Summary:

The latest updates for SIMATIC STEP 7 (TIA Portal) V13 SP1 and SIMATIC STEP 7 (TIA Portal) V12 SP1 fix two vulnerabilities. The more severe of these vulnerabilities could allow Man-in-the-Middle attacks against the Siemens industrial communication protocol.

All vulnerabilities resolved with this software update are discussed below.

AFFECTED PRODUCTS

- SIMATIC STEP 7 (TIA Portal) V13: All versions < V13 SP1 Upd1
- SIMATIC STEP 7 (TIA Portal) V12: All versions < V12 SP1 Upd5

DESCRIPTION

SIMATIC STEP 7 (TIA Portal) is an engineering software tool used to configure and program SIMATIC controllers and Standard PCs running WinAC RTX.

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 client and server could possibly intercept or modify Siemens industrial communications at port 102/tcp and conduct a Man-in-the-Middle attack.

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-2015-1602)

Attackers with read access to TIA project files could possibly reconstruct protection-level passwords or web server passwords.

CVSS Base Score 1.9
CVSS Temporal Score 1.5
CVSS Overall Score 1.5 (AV:L/AC:M/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Mitigating factors

For vulnerability 1, the attacker must have access to the network path between client and server.

For vulnerability 2, the attacker must have local access to the TIA project file.

SOLUTION

Siemens provides Update 1 for SIMATIC STEP 7 (TIA Portal) V13 SP1 [1] and Update 5 for SIMATIC STEP 7 (TIA Portal) V12 SP1 [2] which fix the vulnerabilities.

After applying the update, Siemens strongly recommends to change protection-level and web server passwords.

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 [3] 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.
- Dmitry Sklyarov from PT-Security for coordinated disclosure of vulnerability 2.

ADDITIONAL RESOURCES

[1] Update 1 for SIMATIC STEP 7 (TIA Portal) V13 SP1 can be obtained here:
https://support.industry.siemens.com/cs/ww/en/view/109311724

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

[3] 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

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

[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 (2015-02-17): Publication Date
V1.1 (2015-08-27): Added fix for SIMATIC STEP 7 (TIA Portal) V12 SP1

DISCLAIMER