SSA-234789: Vulnerabilities in SIMATIC STEP 7 (TIA Portal) V13

Publication Date 2015-02-13
Last Update 2015-02-13
Current Version V1.0
CVSS Overall Score 2.0

Summary:

The latest update for SIMATIC STEP 7 (TIA Portal) V13 fixes two vulnerabilities. The vulnerabilities could allow attackers to escalate their privileges under certain conditions. The attacker must have local access to exploit the vulnerabilities.

AFFECTED PRODUCTS

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

DESCRIPTION

SIMATIC STEP 7 (TIA Portal) is an engineering software 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-2015-1355)

Device user passwords in TIA portal project files are stored using a weak hashing algorithm. Attackers with read access to the project file could possibly reconstruct the passwords for device users.

CVSS Base Score 2.1
CVSS Temporal Score 1.6
CVSS Overall Score 1.6 (AV:L/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2015-1356)

Privilege information for device users is stored unprotected in the TIA portal projects. Attackers with access to the project file could possibly read and modify the permissions for device users in the project file. If unsuspecting users are tricked to download the manipulated project files to the device, the user permissions become active.

CVSS Base Score 2.6
CVSS Temporal Score 2.0
CVSS Overall Score 2.0 (AV:L/AC:H/Au:N/C:P/I:P/A:N/E:POC/RL:OF/RC:C)

Mitigating factors

For vulnerability 1 and 2, the attacker must have access to the local system. Additionally for vulnerability 2, unsuspecting users must be tricked to download modified project files to a device (social engineering).

SOLUTION

Siemens provides Service Pack 1 for STEP 7 (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 Aleksandr Timorin from Positive Technologies for coordinated disclosure.

ADDITIONAL RESOURCES

[1] The software update for STEP 7 (TIA Portal) can be obtained here:
http://support.automation.siemens.com/WW/view/en/105825934

[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