SSA-869766: Information Disclosure Vulnerabilities in SIMATIC STEP 7 (TIA Portal) V12 and V13

Publication Date 2016-10-12
Last Update 2016-10-12
Current Version V1.0
CVSS v3.0 Base Score 2.5

SUMMARY

The release of SIMATIC STEP 7 (TIA Portal) V14 fixes two information disclosure vulnerabilities in the storage format of project files. They could allow local attackers to access sensitive information contained in TIA project files under certain conditions.

AFFECTED PRODUCTS

SIMATIC STEP 7 (TIA Portal): All versions < V14

DESCRIPTION

SIMATIC STEP 7 (TIA Portal) is an engineering software to configure and program SIMATIC controllers.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2016-7959)

Local attackers with read access to TIA project files could brute-force pre-shared keys used for machine to machine communication with possibly reduced effort.

CVSS Base Score 2.5
CVSS Vector CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability 2 (CVE-2016-7960)

Local attackers could circumvent the protection of the transport format of TIA Portal project files and potentially access sensitive configuration settings. This format is used by TIA Portal during the migration of project files to a new version (e.g. V12 to V13).

CVSS Base Score 2.5
CVSS Vector CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Mitigating Factors

Access to the TIA project files on engineering workstations or network storage must be protected with appropriate mechanisms from unauthorized access.

SOLUTION

Siemens provides SIMATIC STEP 7 (TIA Portal) V14 [1] which fixes the vulnerabilities and recommends customers migrate projects to the new version.

As a general security measure Siemens strongly recommends to protect network access to the engineering workstations and project storage 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.

ACKNOWLEDGEMENTS

Siemens thanks Dmitry Sklyarov and Gleb Gritsai from Positive Technologies for coordinated disclosure of both vulnerabilities.

ADDITIONAL RESOURCES

[1] SIMATIC STEP 7 (TIA Portal) V14 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109740340

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

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

[4] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-10-12): Publication Date

DISCLAIMER