SSA-621493: Password Storage Vulnerability in SIMATIC STEP7 (TIA Portal)

Publication Date: 2018-11-13
Last Update: 2018-11-13
Current Version: V1.0
CVSS v3.0 Base Score: 4.0

SUMMARY

The latest update for SIMATIC STEP7 (TIA Portal) fixes a vulnerability that could allow an attacker with local access to a project file to reconstruct certain passwords stored in the project.

Siemens recommends to update to the new version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC STEP 7 (TIA Portal): All Versions < V15.1	Update to V15.1 https://support.industry.siemens.com/cs/us/en/view/109758794

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict network access to the engineering station and project storage to trusted sources.
- Restrict access to project files on the engineering station and project storage to trusted users.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

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

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (https://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 CVE-2018-13811

Password hashes with insufficient computational effort could allow an attacker to access to a project file and reconstruct passwords.

The vulnerability could be exploited by an attacker with local access to the project file. No user interaction is required to exploit the vulnerability. The vulnerability could allow the attacker to obtain certain passwords from the project.

At the time of advisory publication no public exploitation of this vulnerability was known.

CVSS v3.0 Base Score	4.0
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2018-11-13): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.