SSA-887801: Information Disclosure Vulnerability in SIMATIC STEP 7 (TIA Portal)

Publication Date: 2023-12-12
Last Update: 2023-12-12
Current Version: V1.0
CVSS v3.1 Base Score: 4.2

SUMMARY

Siemens has released a new version of STEP 7 (TIA Portal) that fixes an information disclosure vulnerability. A local attacker could gain access to the access level password of the SIMATIC S7-1200 and S7-1500 CPUs, when entered by a legitimate user in the hardware configuration of the affected application.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC STEP 7 (TIA Portal): All versions < V19	Update to V19 or later version https://support.industry.siemens.com/cs/ww/en/view/109820994/

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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 3.1 (CVSS v3.1) (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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2022-46141

An information disclosure vulnerability could allow a local attacker to gain access to the access level password of the SIMATIC S7-1200 and S7-1500 CPUs, when entered by a legitimate user in the hardware configuration of the affected application.

CVSS v3.1 Base Score	4.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-316: Cleartext Storage of Sensitive Information in Memory

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Sharon Brizinov from Claroty for reporting the vulnerability

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 (2023-12-12): Publication Date

TERMS OF USE