SSA-350757: Improper Access Control Vulnerability in TIA Portal Affecting S7-1200 and S7-1500 CPUs Web Server (Incl. Related ET200 CPUs and SIPLUS variants)

Publication Date: 2022-04-12
Last Update: 2022-04-12
Current Version: V1.0
CVSS v3.1 Base Score: 6.4

SUMMARY

An attacker could achieve privilege escalation on the web server of certain devices configured by SIMATIC STEP 7 (TIA Portal) due to incorrect handling of the webserver's user management configuration during downloading. This only affects the S7-1200 and S7-1500 CPUs' (incl. related ET200 CPUs and SIPLUS variants) web server, when activated.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC STEP 7 (TIA Portal) V15: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 (TIA Portal) V16: All versions < V16 Update 5	Update to V16 Update 5 or later version https://support.industry.siemens.com/cs/gb/en/view/109775861/ See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 (TIA Portal) V17: All versions < V17 Update 2	Update to V17 Update 2 or later version https://support.industry.siemens.com/cs/gb/en/view/109784441/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Whenever changes of the web server's user configuration are performed with one of the affected versions for S7-1200 or S7-1500 CPUs (incl. related ET200 CPUs and SIPLUS variants), validate web server permissions for unauthenticated users by directly accessing the web server in an unauthenticated manner. In case unauthenticated access is unintentionally possible, the web server's user configuration needs to be removed and reconfigured again using a TIA-Portal V16 Update 5 or V17 Update 2 or later
- In case a new TIA-Portal version is not available, updating the web server's user configuration is not effective in this situation. Instead
  - the PLC must be deleted and reconfigured with a new project. **Warning**: The PLC-program should be copied before deleting the PLC. Or

- the original project (one that was not uploaded by a PLC) should be used to update the web server's user management and to download the changed configuration

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-2021-42029

An attacker could achieve privilege escalation on the web server of certain devices due to improper access control vulnerability in the engineering system software. The attacker needs to have direct access to the impacted web server.

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

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 (2022-04-12): Publication Date

TERMS OF USE