SSA-830194: Missing Authentication Vulnerability in S7-1200 Devices

Publication Date: 2021-08-10
Last Update: 2021-09-14
Current Version: V1.1
CVSS v3.1 Base Score: 8.1

SUMMARY

SIMATIC S7-1200 PLC, version V4.5.0 fails to authenticate against configured passwords when the affected device was provisioned using TIA Portal V13. This could allow an attacker using TIA Portal V13 or later versions to bypass authentication and download arbitrary programs to the PLC.

Siemens has released an update for SIMATIC S7-1200 and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): V4.5.0	Update to V4.5.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109793280/

WORKAROUNDS AND MITIGATIONS

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

- Update to TIA Portal V13 SP1 or any later version before provisioning S7-1200 V4.5.0 devices

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

Products of the SIMATIC S7-1200 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2021-37172

Affected devices fail to authenticate against configured passwords when provisioned using TIA Portal V13. This could allow an attacker using TIA Portal V13 or later versions to bypass authentication and download arbitrary programs to the PLC. The vulnerability does not occur when TIA Portal V13 SP1 or any later version was used to provision the device.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Gao Jian 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 (2021-08-10):	Publication Date
V1.1 (2021-09-14):	Clarified that the use of TIA Portal V13 or later (not only V17 or later) could allow a successful attack

TERMS OF USE