SSA-672373: Vulnerabilities in CP 1543-1 before V2.0.28

Publication Date: 2016-11-18
Last Update: 2022-04-12
Current Version: V1.2
CVSS v3.1 Base Score: 6.6

SUMMARY

SIMATIC CP 1543-1 devices before V2.0.28 contain two vulnerabilities that could allow authorized users to escalate their privileges on the CP or create a denial of service condition.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0): All versions < V2.0.28	Update to V2.0.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109808678/
SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0): All versions < V2.0.28	Update to V2.0.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109808678/

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

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.

The SIMATIC CP 1543-1 communication processor connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption such as FTPs. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

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-2016-8561

Users with elevated privileges to TIA-Portal and project data on the engineering station could possibly get privileged access on affected devices.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-269: Improper Privilege Management

Vulnerability CVE-2016-8562

Under special conditions it was possible to write SNMP variables on port 161/udp which should be read-only and should only be configured with TIA-Portal. A write to these variables could reduce the availability or cause a denial-of-service.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned
- Agence nationale de la sécurité des systèmes d'information (ANSSI) for coordination efforts
- SOGETI for coordinated disclosure

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 (2016-11-18): Publication Date
V1.1 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products
V1.2 (2022-04-12): Updated download link and revised summary section

TERMS OF USE