SSA-672373: Vulnerabilities in SIMATIC CP 1543-1

Publication Date	2016-11-18
Last Update	2016-11-18
Current Version	V1.0
CVSS v3.0 Base Score	6.6

SUMMARY

The latest firmware update for SIMATIC CP 1543-1 devices fixes two vulnerabilities. One of these vulnerabilities could allow authorized users to escalate their privileges on the CP.

AFFECTED PRODUCTS

SIMATIC CP 1543-1: All versions < V2.0.28

DESCRIPTION

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.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (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 Base Score	6.6
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability 2 (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 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

Mitigating Factors

Vulnerability 2 only applies if SNMPv1 is activated or SNMPv3 write access is activated.

SOLUTION

Siemens provides firmware update V2.0.28 [1] for SIMATIC CP 1543-1 devices which fixes the vulnerabilities and recommends customers to update to the new version.

As a general security measure Siemens strongly recommends protecting network access to the management interface of perimeter devices with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- SOGETI for coordinated disclosure of the vulnerabilities
- Agence nationale de la sécurité des systèmes d'information (ANSSI) for coordination efforts

ADDITIONAL RESOURCES

[1] The firmware update V2.0.28 for SIMATIC CP 1543-1 devices can be downloaded here:
https://support.industry.siemens.com/cs/ww/en/view/109743137

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[4] For further inquiries on 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

DISCLAIMER

See: https://www.siemens.com/terms_of_use