SSA-559174: Multiple Vulnerabilities in CP1604 and CP1616 devices

Publication Date: 2019-01-08
Last Update: 2019-07-09
Current Version: V1.1
CVSS v3.0 Base Score: 9.1

SUMMARY

Multiple vulnerabilities have been identified in SIEMENS CP1604 and CP1616 devices. The most severe of these vulnerabilities could allow an attacker to extract internal communication data or cause a Denial-of-Service condition.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
CP 1604: All versions	Update to V2.8 and follow recommendations from Section Workarounds and Mitigations. https://support.industry.siemens.com/cs/ww/en/view/109762689
CP 1616: All versions	Update to V2.8 and follow recommendations from Section Workarounds and Mitigations. https://support.industry.siemens.com/cs/ww/en/view/109762689

WORKAROUNDS AND MITIGATIONS

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

- Disable the integrated web server. The web server is disabled in the default settings and its use is optional. Use in a productive environment is discouraged.
- Restrict access to to the device to the internal or VPN network. Further restrict access to the web interface (80/tcp) and to the telnet port (23/tcp) to trusted IP addresses if possible.
- Do not click on links from unknown sources.
- Fixes for CVE-2018-13808 have also been released in versions V2.5.2.7, V2.6.2.2, V2.7.2.1 and V2.8 of CP 1616 and CP 1604: https://support.industry.siemens.com/cs/ww/en/view/109768664

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

CP 1616 and CP 1604 are PCI/PCI-104 cards for high-performance connection of field devices to Industrial Ethernet with PROFINET.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2018-13808

An attacker with network access to port 23/tcp could extract internal communication data or cause a Denial-of-Service condition.

Successful exploitation requires network access to a vulnerable device.

At the time of advisory publication no public exploitation of this vulnerability was known.

CVSS v3.0 Base Score	9.1
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-13809

The integrated web server of the affected CP devices could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into following a malicious link.

User interaction is required for a successful exploitation.

At the time of advisory publication no public exploitation of this vulnerability was known.

CVSS v3.0 Base Score	6.1
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:T/RC:C

Vulnerability CVE-2018-13810

The integrated configuration web server of the affected CP devices could allow a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link.

Successful exploitation requires user interaction by a legitimate user. A successful attack could allow an attacker to trigger actions via the web interface that the legitimate user is allowed to perform.

At the time of advisory publication no public exploitation of this vulnerability was known.

CVSS v3.0 Base Score	4.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:T/RC:C

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 (2019-01-08): Publication Date
V1.1 (2019-07-09): Update version information and mitigations: add fixes for older product versions for CVE-2018-13808

TERMS OF USE