SSA-940889: Vulnerabilities in the embedded FTP server of SIMATIC CP 1543-1

Publication Date:	2020-02-11
Last Update:	2020-02-11
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8

SUMMARY

The latest update for SIMATIC CP 1543-1 contains two fixes for vulnerabilities within its embedded ProFTPD FTP server. The more severe of these vulnerabilities could allow for remote code execution and information disclosure without authentication.

Siemens has released updates for SIMATIC CP 1543-1 modules.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 1543-1 (incl. SIPLUS NET variants): All Versions >= V2.0 and < V2.2	Update to V2.2 https://support.industry.siemens.com/cs/ww/en/view/109775642

WORKAROUNDS AND MITIGATIONS

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

- Disable the embedded FTP server. The server is deactivated in the default configuration.
- Limit access to port 21/tcp to trusted IP addresses.

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

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.

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-2019-12815

An arbitrary file copy vulnerability in mod_copy of the embedded FTP server allowes for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2019-18217

The embedded FTP server allowes remote unauthenticated denial-of-service due to incorrect handling of overly long commands because execution in a child process enters an infinite loop.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

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 (2020-02-11):	Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.