SSA-679335: Multiple Vulnerabilities in Embedded FTP Server of SIMATIC NET CP Modules

Publication Date: 2021-08-10
Last Update: 2021-08-10
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

SIMATIC CP 1543-1 and CP 1545-1 devices are affected by multiple vulnerabilities in ProFTPD, a third party component, that could allow a remote attacker to access sensitive information and execute arbitrary code.

Siemens has released an update for SIMATIC NET CP 1543-1 and recommends to update to the latest version. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC NET CP 1543-1 (incl. SIPLUS NET variants): All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109800773/
SIMATIC NET CP 1545-1: All versions	See recommendations from section Workarounds and Mitigations

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

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 NET 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.

The SIMATIC NET CP 1545-1 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. 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-2020-9272

ProFTPD 1.3.7 has an out-of-bounds (OOB) read vulnerability in mod_cap via the cap_text.c cap_to_text function, that could lead to information disclosure.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2020-9273

In ProFTPD 1.3.7, it is possible to corrupt the memory pool by interrupting the data transfer channel. This triggers a use-after-free in alloc_pool in pool.c, and possible remote code execution.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-416: Use After Free

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

TERMS OF USE