SSA-253230: Vulnerabilities in SIMATIC S7-1500 CPU family

Publication Date: 2016-02-08
Last Update: 2020-02-10
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

Siemens has released a firmware update for the SIMATIC S7-1500 CPU family which fixes two vulnerabilities. The more severe of these vulnerabilities could allow attackers to cause a Denial-of-Service under certain conditions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V1.8.3	Update to V1.8.3 https://support.industry.siemens.com/cs/de/en/view/109478459

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

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

Products of the SIMATIC S7-1500 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

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-2016-2200

Specially crafted packets sent to port 102/tcp (ISO/TSAP) could cause a Denial-of-Service condition on the affected devices. The CPU will automatically restart and remain in STOP mode. To recover from this condition the CPU needs to be manually put into RUN mode again.

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-20: Improper Input Validation

Vulnerability CVE-2016-2201

The replay protection efficiency at port 102/tcp (ISO/TSAP) of the affected devices could be reduced by remote attackers under certain conditions.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C
CWE	CWE-693: Protection Mechanism Failure

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Lexfo for coordinated disclosure of CVE-2016-2200
- Amossys for coordinated disclosure of CVE-2016-2201
- Agence nationale de la sécurité des systèmes d’information (ANSSI) for coordination efforts
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2016-02-08):	Publication Date
V1.1 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

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.