

SSA-232418: Vulnerabilities in SIMATIC S7-1200 and SIMATIC S7-1500 CPU families

Publication Date: 2019-08-13
 Last Update: 2020-03-12
 Current Version: V1.3
 CVSS v3.1 Base Score: 5.3

SUMMARY

Two vulnerabilities have been identified in the SIMATIC S7-1200 and S7-1500 CPU families. One vulnerability could allow an attacker with network access to affected devices to modify the user program stored on these devices such that the source code differs from the actual running code. The other vulnerability could allow an attacker in a Man-in-the-Middle position to modify network traffic exchanged on port 102/tcp.

Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V20.8	Update to V20.8. Fixes for CVE-2019-10929 are included in the update to version V20.8. For remaining CVEs, see additional recommendations from section Workarounds and Mitigations. https://support.industry.siemens.com/cs/document/109759122/
SIMATIC S7 PLCSIM Advanced: All versions < V3.0	Update to version V3.0. Fixes for CVE-2019-10929 are included in the update to version V3.0. For remaining CVEs, see additional recommendations from section Workarounds and Mitigations. https://support.industry.siemens.com/cs/document/109772889/
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.4	Update to version V4.4. Fixes for CVE-2019-10929 are included in the update to version V4.4. For remaining CVEs, see additional recommendations from section Workarounds and Mitigations. https://support.industry.siemens.com/cs/search?search=S7-1200%20V4.4%20&type=Download

SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants), excluding CPU 1518 MFP (and related SIPLUS variant): All versions < V2.8.1	Update to V2.8.1. Fixes for CVE-2019-10929 are included in the update to version V2.8.1. For remaining CVEs, see additional recommendations from section Workarounds and Mitigations. https://support.industry.siemens.com/cs/document/109478459/
SIMATIC S7-1500 Software Controller: All versions < V20.8	Update to V20.8. Fixes for CVE-2019-10929 are included in the update to version V20.8. For remaining CVEs, see additional recommendations from section Workarounds and Mitigations. https://support.industry.siemens.com/cs/document/109772864/

WORKAROUNDS AND MITIGATIONS

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

- All affected devices contain a feature called “Access Protection” which prohibits unauthorized modifications of user code. Siemens recommends using access protection to protect affected devices from unauthorized modifications.

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 S7-1200 CPU and SIMATIC S7-1500 CPU families have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

SIMATIC S7-PLCSIM Advanced enables you to create virtual controllers for simulating S7-1500 and ET 200SP controllers and provides extensive simulation of functions.

The SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

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-2019-10929

An attacker in a Man-in-the-Middle position could potentially modify network traffic exchanged on port 102/tcp to PLCs of the SIMATIC S7-1200, SIMATIC S7-1500 and SIMATIC SoftwareController CPU families, due to certain properties in the calculation used for integrity protection.

In order to exploit the vulnerability, an attacker must be able to perform a Man-in-the-Middle attack. The vulnerability could impact the integrity of the communication.

No public exploitation of the vulnerability was known at the time of advisory publication.

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:T/RC:C
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Vulnerability CVE-2019-10943

An attacker with network access to port 102/tcp could potentially modify the user program on the PLC in a way that the running code is different from the source code which is stored on the device.

An attacker must have network access to affected devices and must be able to perform changes to the user program. The vulnerability could impact the perceived integrity of the user program stored on the CPU. An engineer that tries to obtain the code of the user program running on the device, can receive different source code that is not actually running on the device.

No public exploitation of the vulnerability was known at the time of advisory publication.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:T/RC:C
CWE	CWE-353: Missing Support for Integrity Check

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Eli Biham, Sara Bitan, Aviad Carmel, and Alon Dankner from Faculty of Computer Science, Technion Haifa for reporting the vulnerabilities
- Uriel Malin and Avishai Wool from School of Electrical Engineering, Tel-Aviv University for reporting the vulnerabilities
- 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 (2019-08-13): Publication Date
- V1.1 (2019-12-10): Added updates for S7-1200 and S7-1500. SIPLUS devices now explicitly mentioned in the list of affected products
- V1.2 (2020-03-10): Removed exclusion of SIMATIC S7-1500 CPU 1518-4 PN/DP. Added patch links for ET200 CPU 1515 SP2 and SIMATIC S7-1500 Software Controller.
- V1.3 (2020-03-12): Fix information about affected versions in product list.

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.