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

Publication Date: 2019-08-13
Last Update: 2022-08-09
Current Version: V1.4
CVSS v3.1 Base Score: 5.3

SUMMARY

Two vulnerabilities have been identified in the SIMATIC S7-1200/S7-1500 CPU families and related products. One vulnerability (CVE-2019-10943) 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 (CVE-2019-10929) 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 to fix CVE-2019-10929 and recommends to update to the latest versions. Regarding CVE-2019-10943, Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Drive Controller family: All versions only affected by CVE-2019-10943	Currently no fix is planned 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 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions >= V20.8 only affected by CVE-2019-10943	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.4.0	Update to V4.4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793280/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions >= V4.4.0 only affected by CVE-2019-10943	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.8.1	Update to V2.8.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions >= V2.8.1 only affected by CVE-2019-10943	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions < V20.8	Update to V20.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109772864/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions >= V20.8 only affected by CVE-2019-10943	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109772889/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions >= V3.0 only affected by CVE-2019-10943	Currently no fix is planned 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:

- Apply password protection for S7 communication

Product specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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

SIMATIC Drive Controllers have been designed for the automation of production machines, combining the functionality of a SIMATIC S7-1500 CPU and a SINAMICS S120 drive control.

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.

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

SIMATIC S7-1500 CPU products 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 simulates S7-1200, S7-1500 and a few other PLC derivatives. Includes full network access to simulate the PLCs, even in virtualized environments.

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

Affected devices contain a message protection bypass vulnerability due to certain properties in the calculation used for integrity protection.

This could allow an attacker in a Man-in-the-Middle position to modify network traffic sent on port 102/tcp to the affected devices.

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-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.

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:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned
- Eli Biham, Sara Bitan, Aviad Carmel, and Alon Dankner from Faculty of Computer Science, Technion Haifa for reporting the vulnerabilities
- Avishai Wool from School of Electrical Engineering, Tel-Aviv University for reporting the vulnerabilities

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 solution for CVE-2019-10929 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 solution for CVE-2019-10929 for ET200SP CPU 1515SP PC2 and SIMATIC S7-1500 Software Controller
V1.3 (2020-03-12):	Fix information about affected versions in product list.
V1.4 (2022-08-09):	Added SIMATIC Drive Controller and SIMATIC ET 200SP Open Controller CPU 1515SP PC as affected products; separate fix information for the different CVE IDs; updated fix release URL for SIMATIC S7-1200; reviewed mitigation measure

TERMS OF USE