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

Publication Date: 2019-08-13
Last Update: 2019-08-13
Current Version: V1.0
CVSS v3.0 Base Score: 5.3

SUMMARY

Two vulnerabilities have been identified in the SIMATIC S7-1200 and the SIMATIC 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 is working on updates and recommends that customers apply mitigations to reduce the risk until updates are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC ET 200SP Open Controller CPU 1515SP PC: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family: All versions >= V4.0	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: 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:

- 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.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2019-10929

An attacker in a Man-in-the-Middle position could potentially modify network traffic exchanged on port 102/tcp, 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 v3.0 Base Score	3.7
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:T/RC:C

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 v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:T/RC:C

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

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

TERMS OF USE