SSA-434534: Memory Protection Bypass Vulnerability in SIMATIC S7-1200 and S7-1500 CPU Families

Publication Date: 2021-05-28
Last Update: 2021-05-28
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

SIMATIC S7-1200 and S7-1500 CPU products contain a memory protection bypass vulnerability that could allow an attacker to write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks.

Siemens has released updates for several affected products and strongly recommends to update to the latest versions. 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 Drive Controller family: All versions < V2.9.2	Update to V2.9.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.5.0	Update to V4.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793280/
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.9.2	Update to V2.9.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 Software Controller: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions < V4.0	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109795016/

WORKAROUNDS AND MITIGATIONS

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

- Apply password protection for S7 communication

- Disallow client connections via the ENDIS_PW instruction of the S7-1200 or S7-1500 CPU (This blocks remote client connections, even when the client can provide the correct password)
- Use the display to configure additional access protection of the S7-1500 CPU (This blocks remote client connections, even when the client can provide the correct password)
- Apply “defense in depth” as outlined on pages 12ff of the operational guidelines for Industrial Security, especially:
  - Plant security: Physical prevention of access to critical components
  - Network security: Ensure that PLC systems are not connected to untrusted networks
  - System integrity: Configure, maintain and protect your device by applying applicable compensating controls and using built-in security capabilities.
- Update your entire solution to TIA Portal V17 and use TLS communication using individual certificates between PLC, HMIs and PG/PC

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 family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

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.

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

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

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.

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-2020-15782

Affected devices are vulnerable to a memory protection bypass through a specific operation.

A remote unauthenticated attacker with network access to port 102/tcp could potentially write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Tal Keren from Claroty for coordinated disclosure

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 (2021-05-28): Publication Date

TERMS OF USE