SSA-865327: Incorrect Authorization Vulnerability in Industrial Products

Publication Date: 2021-08-10
Last Update: 2021-09-14
Current Version: V1.1
CVSS v3.1 Base Score: 5.3

SUMMARY

The latest updates for the below mentioned products fix a vulnerability that allows an unauthenticated attacker to read PLC variables from affected devices without proper authentication under certain circumstances.

Siemens has released updates for some of the affected products, is working on updates for the remaining affected products and recommends specific countermeasures until fixes are 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 < V21.9	Update to V21.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/
SIMATIC S7 PLCSIM Advanced: All versions > V2 < V4	Updated to V4 or later version https://support.industry.siemens.com/cs/de/en/view/109795016
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): Version V4.4	Update to V4.4.1 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 > V2.5 < 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 > V2.5 < V21.9	Update to V21.9 or later version https://support.industry.siemens.com/cs/de/en/view/109478528/
TIM 1531 IRC (incl. SIPLUS NET variants): Version V2.1	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798331

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

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 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.

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 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.

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN networks.

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-2020-28397

Due to an incorrect authorization check in the affected component, an attacker could extract information about access protected PLC program variables over port 102/tcp from an affected device when reading multiple attributes at once.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-863: Incorrect Authorization

ADDITIONAL INFORMATION

This vulnerability has been discovered internally by Siemens.

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 (2021-08-10): Publication Date
V1.1 (2021-09-14): Added solution for SIMATIC ET 200SP Open Controller CPU 1515SP PC2 and SIMATIC S7-1500 Software Controller

TERMS OF USE