

SSA-381684: Improper Password Protection during Authentication in SIMATIC S7-300 and S7-400 CPUs and Derived Products

Publication Date: 2020-09-08
Last Update: 2020-12-08
Current Version: V1.3
CVSS v3.1 Base Score: 5.9

SUMMARY

A vulnerability has been identified in SIMATIC S7-300 and S7-400 CPU families and derived products, which could result in credential disclosure.

Siemens recommends countermeasures as there are currently no fixes available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX (F) 2010: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK 840D sl: 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:

- Apply Defense-in-Depth concept: <https://www.siemens.com/industrialsecurity>
- Apply cell protection concept: <https://www.siemens.com/cert/operational-guidelines-industrial-security>
- For SIMATIC S7-CPU 410 CPUs: Activate Field Interface Security in PCS 7 V9.0, and use a CP443-1 Adv. to communicate with ES/OS

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 Siemens SIMATIC S7-300 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

Products in the SIMATIC S7-400 CPU family have been designed for process control in industrial environments. They are used worldwide, e.g. in the automotive industry, mechanical equipment manufacture, warehousing systems, building engineering, steel industry, power generation and distribution, pharmaceuticals, food and beverages industry, or chemical industry.

SIMATIC WinAC RTX (F) 2010 is a SIMATIC software controller for PC-based automation solutions.

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production 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-2020-15791

The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-522: Insufficiently Protected Credentials

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Hyunguk Yoo from University of New Orleans for reporting the vulnerability
- Irfan Ahmed and Adeen Ayub from Virginia Commonwealth University for reporting the vulnerability
- Jongwon Choi from NSR (National Security Research Institute) for reporting the vulnerability
- Taeshik Shon from Ajou University for reporting the vulnerability

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 (2020-09-08): Publication Date
- V1.1 (2020-10-13): Added SIMATIC WinAC RTX (F) 2010 and SINUMERIK 840D sl to the list of affected products
- V1.2 (2020-11-10): Corrected CVSS Score for CVE-2020-15791
- V1.3 (2020-12-08): Updated the section ACKNOWLEDGMENTS

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.