SSA-763427: Authentication Bypass Vulnerability in SIMATIC NET CP Modules and TIM Devices

Publication Date: 2015-11-27
Last Update: 2021-04-13
Current Version: V1.5
CVSS v3.1 Base Score: 9.8

SUMMARY

Siemens has released updates for Communication Processor (CP) module families CP 343-1/TIM 3V-IE/TIM 4R-IE/CP 443-1 to resolve an authentication bypass vulnerability that could allow unauthenticated users to perform administrative operations under certain conditions.

2021-04-13: Siemens has also added Profibus devices (CP 342-5 / CP 443-5) to this advisory. For these additional devices, the attacker must have network access to S7 Protocol Interface of the affected device and the configuration data of the CP must be stored on the CPU. Therefore, in this case the adapted CVSS Vector is CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (9.6)

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC NET CP 342-5 (incl. SIPLUS variants): All versions	The attacker must have network access to S7 Protocol Interface of the affected device and the configuration data of the CP must be stored on the CPU.
SIMATIC NET CP 343-1 Advanced (incl. SIPLUS variants): All versions < V3.0.44	Update to V3.0.44 https://support.industry.siemens.com/cs/ww/en/view/109480765
SIMATIC NET CP 343-1 Lean (incl. SIPLUS variants): All versions < V3.1.1	Update to V3.1.1 https://support.industry.siemens.com/cs/ww/en/view/109486101
SIMATIC NET CP 343-1 Standard (incl. SIPLUS variants): All versions < V3.1.1	Update to V3.1.1 https://support.industry.siemens.com/cs/ww/en/view/109486101
SIMATIC NET CP 443-1 Advanced (incl. SIPLUS variants): All versions < V3.2.9	Update to V3.2.9 https://support.industry.siemens.com/cs/ww/en/view/109482246
SIMATIC NET CP 443-1 Standard (incl. SIPLUS variants): All versions < V3.2.9	Update to V3.2.9 https://support.industry.siemens.com/cs/ww/en/view/109482246
SIMATIC NET CP 443-5 Basic (incl. SIPLUS variants): All versions	The attacker must have network access to S7 Protocol Interface of the affected device and the configuration data of the CP must be stored on the CPU.

SIMATIC NET CP 443-5 Extended: All versions	The attacker must have network access to S7 Protocol Interface of the affected device and the configuration data of the CP must be stored on the CPU.
TIM 3V-IE / TIM 3V-IE Advanced (incl. SIPLUS NET variants): All versions < V2.6.0	Update to V2.6.0 https://support.industry.siemens.com/cs/ww/en/view/109481769
TIM 3V-IE DNP3 (incl. SIPLUS NET variants): All versions < V3.1.0	Update to V3.1.0 https://support.industry.siemens.com/cs/ww/en/view/109481766
TIM 4R-IE (incl. SIPLUS NET variants): All versions < V2.6.0	Update to V2.6.0 https://support.industry.siemens.com/cs/ww/en/view/109481769
TIM 4R-IE DNP3 (incl. SIPLUS NET variants): All versions < V3.1.0	Update to V3.1.0 https://support.industry.siemens.com/cs/ww/en/view/109482246

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds. Please follow 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

Communication Processor (CP) modules of families SIMATIC NET CP 343-1 and CP 443-1 have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet communication.

Communication Processor (CP) modules of families SIMATIC NET CP 342-5 and CP 443-5 have been designed to enable SIMATIC S7-300/S7-400 CPUs for PROFIBUS DP/ FMS, S5-compatible, PG/OP and S7 communication.

The TIM 3V-IE is a SINAUT ST7 communications module for the SIMATIC S7-300 with an RS232 interface for SINAUT communication via a classic WAN and an RJ45 interface for SINAUT communication via an IP-based network (WAN or LAN).

The TIM 3V-IE DNP3 communication module for SIMATIC S7-300 with an RS232 interface for DNP3 communication via a classic WAN and an RJ45 interface for DNP3 communication via a IP-based network (WAN or LAN).

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-2015-8214

The implemented access protection level enforcement of the affected communication processors (CP) could possibly allow unauthenticated users to perform administrative operations on the CPs if network access (port 102/TCP) is available and the CPs' configuration was stored on their corresponding CPUs.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Lei ChengLin (Z-0ne) from Fengtai Technologies' Security Research Team for coordinated disclosure
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2015-11-27): Publication Date
V1.1 (2016-01-29): Added fix information for SIMATIC TIM 3V-IE and TIM 4R-IE modules
V1.2 (2016-02-01): Added fix information for SIMATIC CP 443-1 / CP 443-1 Advanced
V1.3 (2016-04-29): Added fix information for SIMATIC CP343-1 Lean / CP 343-1
V1.4 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products
V1.5 (2021-04-13): Clarified product names and added SIMATIC NET CP PROFIBUS devices

TERMS OF USE