SSA-273799: Message Integrity Protection Bypass Vulnerability in SIMATIC Products

Publication Date: 2019-12-10
Last Update: 2022-04-12
Current Version: V1.3
CVSS v3.1 Base Score: 3.7

SUMMARY

A message integrity protection bypass vulnerability has been identified in several SIMATIC products. The vulnerability could allow an attacker in a Man-in-the-Middle position to modify network traffic exchanged on port 102/tcp to PLCs of the SIMATIC S7-1200, SIMATIC S7-1500 and SIMATIC SoftwareController CPU families.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 1626 (6GK1162-6AA01): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC HMI Panel (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V14: All versions < V14 SP1 Update 14	Update to V14 SP1 Update 14 or later version https://support.industry.siemens.com/cs/ww/en/view/109807351/
SIMATIC NET PC Software V15: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 (TIA Portal): All versions < V16	Update to version V16 https://support.industry.siemens.com/cs/document/109772803/
SIMATIC WinCC (TIA Portal): All versions < V16	Update to version V16 https://support.industry.siemens.com/cs/document/109772803/
SIMATIC WinCC OA: All versions < V3.16 P013	Update to V3.16 P013 or later version https://www.winccoa.com/downloads/category/versions-patches.html
SIMATIC WinCC Runtime Advanced: All versions < V16	Update to version V16 https://support.industry.siemens.com/cs/document/109771219/
SIMATIC WinCC Runtime Professional: All versions < V16	Update to version V16 https://support.industry.siemens.com/cs/document/109771219/

TIM 1531 IRC (incl. SIPLUS NET variants): All versions < V2.1	Update to V2.1 https://support.industry.siemens.com/cs/document/109774204/

WORKAROUNDS AND MITIGATIONS

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

Please follow the 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

SIMATIC CP 1626 enables SIMATIC PGs/PCs and PCs equipped with a PCI Express slot to be connected to PROFINET IO.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

SIMATIC NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

SIMATIC STEP 7 (TIA Portal) is an engineering software to configure and program SIMATIC controllers.

SIMATIC WinCC (TIA Portal) is an engineering software to configure and program SIMATIC Panels, SIMATIC Industrial PCs, and Standard PCs running WinCC Runtime Advanced or SCADA System WinCC Runtime Professional visualization software.

SIMATIC WinCC Open Architecture (OA) is part of the SIMATIC HMI family. It is designed for use in applications requiring a high degree of customer-specific adaptability, large or complex applications and projects that impose specific system requirements or functions.

SIMATIC WinCC Runtime Advanced is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC WinCC Runtime Professional is a visualization runtime platform used for operator control and monitoring of machines and plants.

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-2019-10929

Affected devices contain a message protection bypass vulnerability due to certain properties in the calculation used for integrity protection.

This could allow an attacker in a Man-in-the-Middle position to modify network traffic sent on port 102/tcp to the affected devices.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm

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
- Avishai Wool and Uriel Malin 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 (2019-12-10):	Publication Date
V1.1 (2020-02-11):	Added solution for TIM 1531 IRC and SIMATIC NET PC Software
V1.2 (2020-03-10):	Added links for WinCC Runtime
V1.3 (2022-04-12):	Added solution for SIMATIC NET PC Software V14 and clarified affected versions; Clarified no remediation planned

TERMS OF USE