SSA-711829: Denial of Service Vulnerability in TIA Administrator

Publication Date: 2022-04-12
Last Update: 2022-07-12
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

In conjunction with the installation of the affected products listed in the table below, a vulnerability in TIA Administrator occurs that could allow an unauthenticated attacker to perform a denial of service attack.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS neo (Administration Console): All versions < V3.1 SP1	Update to V3.1 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807752/ Apply measures described in “Industrial Security in SIMATIC PCS neo": https://support.industry.siemens.com/cs/ww/en/view/109771524/ See further recommendations from section Workarounds and Mitigations
SINETPLAN: All versions	Update TIA Administrator to V1.0 SP7 or later version https://support.industry.siemens.com/cs/ww/en/view/114358/ See further recommendations from section Workarounds and Mitigations
TIA Portal: V15, V15.1, V16 and V17	Update TIA Administrator to V1.0 SP7 or later version https://support.industry.siemens.com/cs/ww/en/view/114358/ See further 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:

- Restrict access to port 8888/tcp to localhost (default)

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 PCS neo is a distributed control system (DCS).

The Siemens Network Planner (SINETPLAN) supports you as a planner of automation systems based on PROFINET. It facilitates the professional planning, calculation, and simulation of load in a PROFINET network and supports virtual commissioning of the network. SINETPLAN provides the capability to efficiently plan and layout PROFINET networks. It supports both "non-real-time communication", such as when TCP/IP data is used, as well as real-time (RT) or IRT communication.

TIA Administrator is a web-based framework that can incorporate different function modules for administrative tasks, as well as functions for managing SIMATIC software and licenses.

The Totally Integrated Automation Portal (TIA Portal) is a PC software that provides access to the complete range of Siemens digitalized automation services, from digital planning and integrated engineering to transparent operation.

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-2022-27194

The affected system cannot properly process specially crafted packets sent to port 8888/tcp. A remote attacker could exploit this vulnerability to cause a Denial-of-Service condition. The affected devices must be restarted manually.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Peter Cheng from Elex Feigong Research Institute 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 (2022-04-12):	Publication Date
V1.1 (2022-07-12):	Added fix for SINETPLAN and TIA Portal

TERMS OF USE