SSA-428051: Privilege Escalation Vulnerability in TIA Administrator

Publication Date: 2021-02-09
Last Update: 2021-09-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.8

SUMMARY

The latest update for TIA Administrator, installed together with TIA Portal and PCS neo, fixes a privilege escalation vulnerability that could allow local users to escalate privileges and execute code as local SYSTEM user.

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
PCS neo (Administration Console): All versions < V3.1	Update to V3.1 or later version To obtain SIMATIC PCS neo V3.1 contact your local customer support.
TIA Portal: V15, V15.1 and V16	Update TIA Administrator to V1.0 SP2 Upd2 or later version https://support.industry.siemens.com/cs/ww/en/view/114358/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict local access to authorized users.
- For PCS neo apply measures described in “Industrial Security in SIMATIC PCS neo”: https://support.industry.siemens.com/cs/ww/en/view/109771524

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 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.

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.

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-2020-25238

Manipulating certain files in specific folders could allow a local attacker to execute code with SYSTEM privileges.

The security vulnerability could be exploited by an attacker with a valid account and limited access rights on the system.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Will Dormann from CERT Coordination Center (CERT/CC) 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 (2021-02-09):	Publication Date
V1.1 (2021-09-14):	Added solution for SIMATIC PCS neo

TERMS OF USE