SSA-573669: Multiple Vulnerabilities in TIA Administrator Before V3.0.6

Publication Date: 2025-07-08
Last Update: 2025-07-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 8.5

SUMMARY

Siemens TIA Administrator before V3.0.6 contains multiple vulnerabilities which could allow an attacker to escalate privilege or exceute arbitrary code during installations.

Siemens has released a new version for TIA Administrator and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
TIA Administrator: All versions < V3.0.6 affected by all CVEs	Update to V3.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109825038/

WORKAROUNDS AND MITIGATIONS

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

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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2025-23364

The affected application improperly validates code signing certificates. This could allow an attacker to bypass the check and exceute arbitrary code during installations.

CVSS v3.1 Base Score	6.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CVSS v4.0 Base Score	6.9
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N
CWE	CWE-347: Improper Verification of Cryptographic Signature

Vulnerability CVE-2025-23365

The affected application allows low-privileged users to trigger installations by overwriting cache files and modifying the downloads path. This would allow an attacker to escalate privilege and exceute arbitrary code.

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
CVSS v4.0 Base Score	8.5
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-284: Improper Access Control

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 (2025-07-08): Publication Date

TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.