

SSA-116924: Path Traversal Vulnerability in TIA Portal

Publication Date: 2023-04-11
 Last Update: 2024-08-13
 Current Version: V1.2
 CVSS v3.1 Base Score: 7.3

SUMMARY

TIA Portal contains a path traversal vulnerability that could allow the creation or overwrite of arbitrary files in the engineering system. If the user is tricked to open a malicious PC system configuration file, an attacker could exploit this vulnerability to achieve arbitrary code execution.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Totally Integrated Automation Portal (TIA Portal):	See below See recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V15: All versions affected by CVE-2023-26293	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V16: All versions < V16 Update 7 affected by CVE-2023-26293	Update to V16 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861/ See further recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V17: All versions < V17 Update 6 affected by CVE-2023-26293	Update to V17 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109784441/ See further recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V18: All versions < V18 Update 1 affected by CVE-2023-26293	Update to V18 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109817218/ 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:

- Do not open untrusted project files or PC system configuration files

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

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 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-2023-26293

Affected products contain a path traversal vulnerability that could allow the creation or overwrite of arbitrary files in the engineering system. If the user is tricked to open a malicious PC system configuration file, an attacker could exploit this vulnerability to achieve arbitrary code execution.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Michael Heinzl for reporting and 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 (2023-04-11): Publication Date
V1.1 (2023-05-09): Added fix for Totally Integrated Automation Portal (TIA Portal) V17
V1.2 (2024-08-13): Added fix for Totally Integrated Automation Portal (TIA Portal) V16

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.