SSA-116924: Path Traversal Vulnerability in TIA Portal

Publication Date: 2023-04-11
Last Update: 2023-05-09
Current Version: V1.1
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 an update for TIA Portal V18 and recommends to update to the latest version. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

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

TERMS OF USE