

SSA-640968: Untrusted Search Path Vulnerability in TIA Project-Server formerly known as TIA Multiuser Server

Publication Date: 2023-02-14
 Last Update: 2023-05-09
 Current Version: V1.1
 CVSS v3.1 Base Score: 6.7

SUMMARY

TIA Project-Server formerly known as TIA Multiuser Server contains an untrusted search path vulnerability that could allow an attacker to escalate privileges, when tricking a legitimate user to start the service from an attacker controlled path.

Siemens has released updates for several affected products and recommends to update to the latest versions. 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
TIA Multiuser Server V14: All versions	Currently no fix is planned Migrate to TIA Project-Server V1.1 or later version See further recommendations from section Workarounds and Mitigations
TIA Multiuser Server V15: All versions < V15.1 Update 8	Update to V15.1 Update 8 or later version https://support.industry.siemens.com/cs/ww/en/view/109763893/ Migrate to TIA Project-Server V1.1 or later version See further recommendations from section Workarounds and Mitigations
TIA Project-Server V16: All versions	Currently no fix is available Migrate to TIA Project-Server V1.1 or later version See further recommendations from section Workarounds and Mitigations
TIA Project-Server V17: All versions < V17 Update 6	Update to V17 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109800915/ Migrate to TIA Project-Server V1.1 or later version See further recommendations from section Workarounds and Mitigations
TIA Project-Server : All versions < V1.1	Update to V1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810588/ 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:

- Make sure that the directory that is set as working directory when starting the TIA Project-Server or TIA Multiuser Server does not contain untrusted 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

TIA Project-Server formerly known as TIA Multiuser Server allows to work with multiple users together and simultaneously on a project.

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-2022-35868

Affected applications contain an untrusted search path vulnerability that could allow an attacker to escalate privileges, when tricking a legitimate user to start the service from an attacker controlled path.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-426: Untrusted Search Path

ADDITIONAL INFORMATION

Previous versions of the TIA Project-Server or Multiuser Server were delivered together with the TIA Portal from V14. These are the following server versions: Multiuser-Server V14,V14 SP1, V15 and V15.1 as well as TIA Project-Server V16 and V17.

The TIA Project-Server version does not follow the TIA Portal version anymore and the version numbering started with version V1.0 again.

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 (2023-02-14): Publication Date
V1.1 (2023-05-09): Added fix for TIA Project-Server V17

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.