SSA-656895: Open Redirect Vulnerability in Teamcenter

Publication Date:	2025-02-11
Last Update:	2025-02-25
Current Version:	V1.1
CVSS v3.1 Base Score:	7.4
CVSS v4.0 Base Score:	6.1

SUMMARY

The SSO login service in Teamcenter contains an open redirect vulnerability that could allow an attacker to redirect the legitimate user to an attacker-chosen URL to steal valid session data.

Siemens is preparing fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Teamcenter: All versions affected by CVE-2025-23363	Currently no fix is available 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:

- CVE-2025-23363: Do not click on links from untrusted sources

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

Teamcenter software is a modern, adaptable product lifecycle management (PLM) system that connects people and processes, across functional silos, with a digital thread for innovation.

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-2025-23363

The SSO login service of affected applications accepts user-controlled input that could specify a link to an external site. This could allow an attacker to redirect the legitimate user to an attacker-chosen URL to steal valid session data. For a successful exploit, the legitimate user must actively click on an attacker-crafted link.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N
CVSS v4.0 Base Score	6.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:H/SI:N/SA:N
CWE	CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Nicolo Vinci for reporting the vulnerability

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 (2025-02-11):	Publication Date
V1.1 (2025-02-25):	Removed fix version information as the implemented fix was insufficient - final fix being worked on for future release(s)

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.