SSA-987403: Multiple Vulnerabilities in Teamcenter

Publication Date:	2021-09-14
Last Update:	2021-09-14
Current Version:	V1.0
CVSS v3.1 Base Score:	7.2

SUMMARY

Teamcenter is affected by three vulnerabilities namely incorrect privilege assignment, Insecure Direct Object Reference (IDOR) and XML External Entity Injection (XXE).

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Teamcenter V12.4: All versions < V12.4.0.8	Update to V12.4.0.8 or later version https://support.sw.siemens.com/ (login required)
Teamcenter V13.0: All versions < V13.0.0.7	Update to V13.0.0.7 or later version https://support.sw.siemens.com/ (login required)
Teamcenter V13.1: All versions < V13.1.0.5	Update to V13.1.0.5 or later version https://support.sw.siemens.com/ (login required)
Teamcenter V13.2: All versions < 13.2.0.2	Update to V13.2.0.2 or later version https://support.sw.siemens.com/ (login required)

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Avoid to open untrusted files in Teamcenter
- Harden the application's host to prevent local access by untrusted personnel

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 provides a digital twin of products to help the analysis and predict performance before investment in physical parts and production.

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-2021-40354

The “surrogate” functionality on the user profile of the application does not perform sufficient access control that could lead to an account takeover. Any profile on the application can perform this attack and access any other user assigned tasks via the “inbox/surrogate tasks”.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-267: Privilege Defined With Unsafe Actions

Vulnerability CVE-2021-40355

The affected application contains Insecure Direct Object Reference (IDOR) vulnerability that allows an attacker to use user-supplied input to access objects directly.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-639: Authorization Bypass Through User-Controlled Key

Vulnerability CVE-2021-40356

The application contains a XML External Entity Injection (XXE) vulnerability. This could allow an attacker to view files on the application server filesystem.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-611: Improper Restriction of XML External Entity Reference

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Nicolas Verdier from TEHTRIS for reporting the vulnerabilities

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 (2021-09-14): Publication Date

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.