SSA-622535: Multiple Vulnerabilities in Teamcenter Active Workspace

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
CVSS v3.1 Base Score: 6.1

SUMMARY

Multiple vulnerabilities affecting Teamcenter Active Workspace could lead to sensitive information disclosure and reflected cross site scripting.

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 Active Workspace V4: All versions < V4.3.9	Update to V4.3.9 or later version https://support.sw.siemens.com/ (login required)
Teamcenter Active Workspace V5.0: All versions < V5.0.7	Update to V5.0.7 or later version https://support.sw.siemens.com/ (login required)
Teamcenter Active Workspace V5.1: All versions < V5.1.4	Update to V5.1.4 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 from unknown sources in Teamcenter Active Workspace

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 Active Workspace is a web application for accessing the Teamcenter system that provides an identical and seamless experience on any computer or smart device.

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-2021-33711

The affected application allows verbose error messages which allow leaking of sensitive information, such as full paths.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-209: Generation of Error Message Containing Sensitive Information

Vulnerability CVE-2021-33710

A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected devices that could allow an attacker to execute malicious JavaScript code by tricking users into accessing a malicious link.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2021-33709

By sending malformed requests, a remote attacker could leak an application token due to an error not properly handled by the system.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

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 (2021-07-13):   Publication Date

TERMS OF USE