SSA-133772: Zip Path Traversal Vulnerability in Teamcenter Active Workspace

Publication Date: 2021-12-14
Last Update: 2021-12-14
Current Version: V1.0
CVSS v3.1 Base Score: 6.8

SUMMARY

A zip path traversal vulnerability in Teamcenter Active Workspace could allow an attacker to achieve remote code execution.

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 V4.3: All versions < V4.3.11	Update to V4.3.11 or later version https://support.sw.siemens.com/ (login required) See further recommendations from section Workarounds and Mitigations
Teamcenter Active Workspace V5.0: All versions < V5.0.10	Update to V5.0.10 or later version https://support.sw.siemens.com/ (login required) See further recommendations from section Workarounds and Mitigations
Teamcenter Active Workspace V5.1: All versions < V5.1.6	Update to V5.1.6 or later version https://support.sw.siemens.com/ (login required) See further recommendations from section Workarounds and Mitigations
Teamcenter Active Workspace V5.2: All versions < V5.2.3	Update to V5.2.3 or later version https://support.sw.siemens.com/ (login required) 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:

- Harden the application 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 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-2021-41547

The application contains an unsafe unzipping pattern that could lead to a zip path traversal attack. This could allow and attacker to execute a remote shell with admin rights.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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 (2021-12-14): 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.