SSA-789162: Vulnerabilities in Teamcenter

Publication Date: 2022-05-10
Last Update: 2022-05-10
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Teamcenter is affected by XML External Entity Injection (XXE, CVE-2022-29801) and a stack based buffer overflow vulnerability (CVE-2022-24290). XXE impacts only Teamcenter versions before V13.1.

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
Teamcenter V12.4: All versions < V12.4.0.13	Update to V12.4.0.13 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter V13.0: All versions < V13.0.0.9	Update to V13.0.0.9 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter V13.1: All versions only affected by CVE-2022-24290	Currently no fix is available See recommendations from section Workarounds and Mitigations
Teamcenter V13.2: All versions < V13.2.0.8 only affected by CVE-2022-24290	Update to V13.2.0.8 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter V13.3: All versions < V13.3.0.3 only affected by CVE-2022-24290	Update to V13.3.0.3 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter V14.0: All versions only affected by CVE-2022-24290	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:

- Harden the application's host to prevent local access by untrusted personnel

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

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 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-2022-24290

The tcserver.exe binary in affected applications is vulnerable to a stack overflow condition during the parsing of user input that may lead the binary to crash.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2022-29801

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:

- Han Lee from Apple Information Security 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 (2022-05-10): Publication Date

TERMS OF USE