SSA-220589: Hard Coded Default Credential Vulnerability in Teamcenter

Publication Date: 2022-06-14
Last Update: 2022-08-09
Current Version: V1.2
CVSS v3.1 Base Score: 9.9

SUMMARY

Siemens has released updates for Teamcenter that fixes a security vulnerability related to unsecure storage of user credentials. This vulnerability affects Java EE Server Manager HTML Adaptor. This service is not installed by default and currently also obsoleted.

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 < V12.4.0.13	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 < V13.1.0.9	Update to V13.1.0.9 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter V13.2: All versions < V13.2.0.9	Update to V13.2.0.9 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	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 < V14.0.0.2	Update to V14.0.0.2 or later version https://support.sw.siemens.com/ 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's host to prevent local access by untrusted personnel
- Limit access to port 8082/tcp to specific IP addresses, e.g. with a firewall
- Java EE Server Manager HTML Adaptor is obsoleted. It is recommended to use Teamcenter Management Console for Server Manager administration

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-2022-31619

Java EE Server Manager HTML Adaptor in Teamcenter consists of default hardcoded credentials. Access to the application allows a user to perform a series of actions that could potentially lead to remote code execution with elevated permissions.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-798: Use of Hard-coded Credentials

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Han Lee and Matthias Kaiser 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 (2022-06-14):	Publication Date
V1.1 (2022-07-12):	Updated acknowledgment
V1.2 (2022-08-09):	Added remediation for Teamcenter version lines V13.2 and V14.0

TERMS OF USE