TeamConnect® Enterprise 6.3.7 Patch Bundle 5

Release Notes

TCE 6.3.7 Patch Bundle 5 (PTC6370005) resolves the following issues:

Issue: Additional Approver is unable to adjust line items.
Tracking Code: SUPPORTPRI-67529
Case Number: 2023-0525-7855881
Reported Version: TCE 6.3.7

Workaround
No.

Pre-Requisites
- TCE 6.3.7
- Use legacy views for line items.

Steps to Reproduce
- Create an invoice.
- As an approver, add an additional approver.
- Log in as an additional approver. Unable to make line item adjustments.

Expected Results of Steps
Adjust option should be visible to additional approvers just as original approver (This functionality works fine on interactive line item view. However, the user is preferring the legacy view due to some internal reasons).

Actual Results of Steps
Adjust option is not visible to additional approvers.

Root Cause Analysis
Update allowed permission is not carried out to additional approval.

Issue: Session ID is shown in the logs which can impact security.
Tracking Code: SUPPORTPRI-67999
Case Number: 2023-0627-7893213
Reported Version: TCE 6.3.7

Workaround
Disabling the audit rule is insufficient for the user as they worry this can be enabled on the front end as part of an attempt to hijack another user's session.

Pre-Requisites

- Admin / Logging / Audit
- Enable - "Login/ Sign Off"

Steps to Reproduce

1. Log into the TC application and log back out.
2. Log back into TC application once again.
3. Navigate to Admin > Logging > Audit.
4. Open Audit log.

Expected Results of Steps
Login and Logout details are shown, but nothing that could impact security.

Actual Results of Steps
The current session's session ID is displayed. This is not good. The previous session's session ID is displayed - ideally, we should not log this at all.

Root Cause Analysis
Session id is logged.

NOTE : Added a new property 'app.maskSessionId' in teamconnect.properties file, if 'app.maskSessionId' set it to true then session id will be masked or if 'app.maskSessionId' set to false it will display unmasked session id.

Below fixes were merged in from TCE 6.2.4 Patch 12

Issue: TeamConnect Vulnerability Detected when performing actions using gwt.
Tracking Code: SUPPORTPRI-66990
Case Number: 2022-0927-988450
Reported Version: TCE 6.2.4

The fixes in this patch will be merged into TCE 7.1.

INSTALLATION

Important: Stop your TeamConnect® instance before updating any files in the TeamConnect® war file.

1. Update WAR file

Windows GUI:
· Extract patch directory from the .zip file.
· Open the TeamConnect® .war file with 7zip
· Drag and Drop the files from patch directory to .war root in 7zip
· Overwrite file conflicts in 7zip

· Redeploy .war

Windows CMD:

· tar -xf <path_to_patch_zip>
· cd <path_to_extracted_directory>
· jar -uvf <path_to_war> .\
· Redeploy .war

Linux Terminal:

· unzip <path_to_patch_zip> -d <path_to_destination_folder>
· cd <path_to_destination_folder>
· jar -uvf <path_to_war> .\
· Redeploy .war

2. Update database and version information

Use the following steps to update the database and add patch version information to the **About** page of the **Admin Settings**.

1. Stop the TeamConnect® instance if it is currently running.
2. Backup your TeamConnect® database.
3. Run the script, located in **\update**, that is appropriate for your database server:
    - MSSQL_TeamConnect_637_PB5.sql
    - ORACLE_TeamConnect_637_PB5.sql
4. Restart TeamConnect®.

UPGRADE CONSIDERATION

No significant upgrade considerations for this patch.

LEVEL OF RISK TO UPDATE WITH PATCH

LOW