Plugin Review

local_repositoryfileupload

For

University College London

by

Catalyst IT Europe Limited

Version: 1.0

November 2020

Commercial in Confidence

open source technologists

Olivier House, 18 Marine Parade, Brighton, East Sussex, BN2 1TL, United Kingdom
+44 (0) 1273 929 450 // info@catalyst-eu.net // www.catalyst-eu.net

Table of Contents

Revision History			
Modified By	**Date**	**Version**	**Change**
Conn Warwicker	12 November 2020	1.0	Retrospective Review

1 Introduction

1.1 Overview

The following review of the local_repositoryfileupload plugin has been carried out in accordance with our Code and Deployment Process Standard.

1.2 Summary

The plugin local_repositoryfileupload falls into the ● **medium risk (amber)** category due to potential security issues, code falling outside of Moodle standards and the potential for disk space running out. This means it needs approval from University College London before release.

About Our Plugin Review Risk Ratings

● **Low Risk (Green)**

The plugin is free from any noticeable issues. Performance impacts are unlikely and no security threats are present. The plugin is well maintained by the third party maintainer.

Plugin may be deployed to your service.

● **Medium Risk (Amber)**

The plugin review has presented concerns or issues with the plugin. It may show potential performance issues or be poorly maintained by the third party maintainer.

The plugin may be released to your service but Catalyst reserve the right to remove it without warning and without permission, should it place our SLA at risk.

● **High Risk (Red)**

The plugin review has identified issues in the plugin, most likely related to security or performance. You will receive clear reasoning in your plugin review document.

The plugin is not authorised for use on your service until issues are fixed.

1.3 Plugin Overview

The local_repositoryfileupload plugin appears to be a plugin which (depending on permissions) allows a user to manually upload a file to a File System repository, or delete a file from said repository. This is achieved by providing a link in the course settings navigation to the local upload form, if the course has an instance of the repository confgured.

Item	Result
Version	2018032300
Release	N/A
Requires	2017110800
Usage	N/A
Author/copyright holder	UCL
Online reviews	N/A
Compatibility	N/A

2 Review Results

2.1 Security

The following potential issues were found:

- The navigation link to the form uses a capability check of moodle/backup:backupcourse to see if the user should see the link or not, however the form itself requires the *local/repositoryfileupload:upload* and *local/repositoryfileupload::delete* capabilities. This is not a major issue, as access to the forms will still be restricted, but users may be able to see the link when they shouldn't be able to.
- Some files missing MOODLE_INTERNAL check.
- Some uses of $_POST instead of using moodle's required/optional_param functions.
- Use of manual *move_uploaded_files* instead of using moodle's form and file APIs.

It does not appear to be possible to upload or delete any files which we should not be able to, however, in general it would still be better to use Moodle's APIs for the forms and file manipulations.

Item	Result
Permissions	OK, except for navigation link using wrong capability check.
Authentication	OK – require_login called on pages where relevant.
Form inputs	Some use of direct $_POST variables, however does not appear to be used in any database queries.
Other inputs	N/A
External data in HTML	N/A
Cross site scripting	N/A

Item	Result
SQL parametrised	OK - Database queries use Moodle’s database API.
Data exposure	OK
Shell commands	OK
CSRF	Rather than using Moodle’s forms with in-built sesskey checks, this plugin has implemented its own version. It appears to work, though would probably be better to stick to the Moodle standard.
Data leakage	OK
Transmission to third parties	OK

2.2 Coding Quality

Coding quality is acceptable, though the plugin was obviously written a while ago. Commenting is generally okay and found in most functions/methods.

Item	Result
Outstanding bugs upstream	N/A
Installation	OK
Notices seen	No notices observed.
Basic functionality	Basic file upload and deletion functionality appears to work. No exploits observed.
Admin functionality	N/A
Backup	N/A
Restored	N/A
Removed	OK
Coding standards violations	A TOTAL OF 79 ERRORS AND 86 WARNINGS WERE FOUND IN 8 FILES
Abstraction	Abstraction is generally okay. Plugin makes use of classes and objects. Functions are not particularly long.
Unit testing	Not checked
Side effects	No side effects observed.
Code documentation	Commenting across the plugin is acceptable, though could use a tidy up and update to docblocks.

2.3 Performance

No performance issues noted in the basic use of the plugin. However, if the user is attempting to upload a very large file, this could potentially slow things down and may lead to their session timing out.

Item	Result
Really big synchronous jobs	N/A
Database killing queries	N/A
Page response time	N/A
Disk usage	Plugin allows for the uploading of files directly to the File System. Whilst this isn't a problem, it means if users start uploading lots of big files, the disk may run out of space fairly rapidly, depending on available space.

3 Review Environment

Item	Result
Plugin name	local_repositoryfileupload
Plugin git hash	dfdfc0dd52e61ac0151d72ae44aa4217719f0012
Plugin upstream repository	https://git.catalyst-eu.net/ucl/moodle-local_repositoryfileupload
Plugin repository	ssh://reviews.ci.catalyst-eu.net:29418/moodle-local_repositoryfileupload
Main git hash	7a7da0ff195800fe991af23df8c59d467361 62a6
Main git repo	ssh://reviews.ci.catalyst-eu.net:29418/moodle
Database version	mysql (5.7.27-0ubuntu0.18.04.1)
Database character encoding	utf8
Database dump date	N/A
Site data dump date	N/A