Plugin Review

block_portico_enrolments

For

UCL

by

Catalyst IT Europe Limited

Version: 1.0

February 2021

Commercial in Confidence

catalyst

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	16 Feb 2021	1.0	Initial Retroactive Review

Introduction

Overview

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

Summary

The plugin block_portico_enrolments falls into the ● **High Risk (Red)** category due to security issues, outlined in Security section. This means the plugin is not authorised for use on your service until these issues are resolved.

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.

Plugin Overview

From the README file:
"A Moodle block that maps your course to Portico Module occurrences, departments, faculties, programmes and routes.

This block displays any mapping that is done to your course in a block once editing is turned on in a course. If no mappings are displayed then you can click an edit Portico enrolments link to add or edit previous mappings."

This plugin is already installed on the production system, so this is a retroactive review.

Due to the nature of the plugin – syncing data between the external Portico system, we will be unable to test the actual functionality.

Item	Result
Version	2018083100
Release	2.4 (Build: 2018083100)
Requires	2013110500 (Moodle 2.6)
Usage	UCL
Author/copyright holder	UCL
Online reviews	N/A
Compatibility	Unknown

Review Results

Security

General
- Various files make direct use of $_POST. This should be replaced with either optional_param() or required_param().

view.php
- There do not appear to be any capability checks here, only require_login(). So any students on the course could access this URL directly and run the search in the included ajax.php file, presumably.

insert.php
- There do not appear to be any capability or login checks here. So anyone in the world who $POSTs to the URL directly could insert/delete data in your database.

Item	Result
Permissions	MISSING – There are several files where there are no capability checks done, which means in some cases students could access datsa they shouldn't be able to, and in another case, anyone who submits a POST request to the URL could alter data in the database.
Authentication	MISSING – There are some files which do not check for authentication to Moodle, meaning they are open to the outside world.
Form inputs	OK

Item	Result
Other inputs	OK – Database queries all appear to use the standard prepared statements with placeholder values.
External data in HTML	Unknown – We are unable to check the actual data being returned from the external database, however it is quite possible that it is not being escaped properly, due to the custom template being used.
Cross site scripting	OK
SQL parametrised	Database queries all appear to use the standard prepared statements with placeholder values. However, variables are used in lots of places for table names or column names, so care should be taken to ensure none of those come from user-submitted data. None were noticed, but it is possible that some were overlooked.
Data exposure	Due to the lack of login and capability checks on some pages, some data could be exposed to users who should not have access to it.
Shell commands	N/A
CSRF	Database queries are run solely on process of $_POST request, with no additional checks. Once the $_POST references are changed to use moodle's optional/required params, then the session checks should also be added in to avoid csrf.
Data leakage	Unknown
Transmission to third parties	N/A

Coding Quality

In general, the code is quite old and clearly did not go through any kind of review process, as there is lots of commented out code and debugging statements. The code is generally done in a procedural way, rather than making use of classes. It also has lots of coding standards violations, some of which are minor, but some of which are important and should be addressed ASAP.

Recommendations

If you want to update the plugin to more match the current Moodle standards, the following would be the recommendations to consider:

- Go through the codechecker results (attached to WR348550) and address all of the errors and warnings.
- Run the moodlecheck documentation checker and resolve any issues.
- Remove the .phtml file and your custom templating code and move HTML content to use a Mustache template
- Remove the jscp directory and move javascript to AMD modules.
- Remove references to $_GET/$_POST and replace with optional_param() or required_param()

- You do not need to call the $PAGE→requires→jquery() method any more, as if you use an AMD module, you can tell your module to require jquery.
- Tidy up commented-out code
- Generally in Moodle require_once() is used, not include()
- Tidy up some long procedural files, e.g. insert.php and move functionality to classes and methods, which is easier to manage and document.
- Tidy up SQL queries.
- Remove logic from settings.php file. That should just be used to define Moodle settings for your plugin, not to run any queries. If you wish to have custom settings which require running queries, they should be in a separate file.
- If you run some action (e.g. a database update) from the POST of a file, and you are not using Moodle forms, you should always make sure that the user's session is submitted along with it, to avoid cross site forgery.

Item	Result
Outstanding bugs upstream	N/A
Installation	Not checked (Plugin is already installed on production)
Notices seen	N/A – Unable to test functionality, due to external database connection.
Basic functionality	N/A – Unable to test functionality, due to external database connection.
Admin functionality	N/A – Unable to test functionality, due to external database connection.
Backup	N/A – Unable to test functionality, due to external database connection.
Restored	N/A – Unable to test functionality, due to external database connection.
Removed	N/A – Unable to test functionality, due to external database connection.
Coding standards violations	A TOTAL OF 152 ERRORS AND 271 WARNINGS WERE FOUND IN 9 FILES
Abstraction	Abstraction is poor and plugin could do with being re-factored.
Unit testing	N/A
Side effects	Unknown, but unlikely based on the code review.
Code documentation	Most files are well commented. There is a lot of old code commented out which should be removed.

Performance

Due to the functionality requiring a connection to the external Student Information Systems database, performance could not be checked. However, some recommendations have been made, based on reviewing the code alone.

Item	Result
Really big synchronous jobs	OK – None noticed.
Database killing queries	Unable to test, due to external database connection. However, looking at the queries themselves, there does not appear to be any massive queries which would cause problems. It should be noted though, that queries to the external database are done every time the block loads, so if there is a problem with the external database, this could potentially slow/kill the course page. It may be worth investigating this and seeing if there is another way this could be done.
Page response time	N/A – Unable to test functionality, due to external database connection.
Disk usage	OK – Plugin does not appear to do anything which would affect the storage disk.

Review Environment

Item	Result
Plugin name	block_portico_enrolments
Plugin git hash	afaaaf8ec1064c95263a18121c39c219bea8d78a
Plugin upstream repository	git@git.catalyst-eu.net:ucl/moodle-block_portico_enrolments.git
Plugin repository	git@git.catalyst-eu.net:ucl/moodle-block_portico_enrolments.git
Main git hash	0fb459175246aaca4cdae983bb007a9f34de4b20
Main git repo	git@git.catalyst-eu.net:ucl/moodle.git
Database version	mysqlnd 5.0.12-dev - 20150407
Database character encoding	utf-8
Database dump date	N/A
Site data dump date	N/A