Plugin Review

enrol_dbuserrel

For

University College London

by

Catalyst IT Europe Limited

Version: 1.0

November 2020

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	13 November 2020	1.0	Retrospective Review

1 Introduction

1.1 Overview

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

1.2 Summary

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

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 enrol_dbuserrel plugin appears to be an enrolment plugin which allows the syncing of mentor/mentee relationships from an external database, by mapping database fields to Moodle user fields and roles. Given an external table with columns for *student*, *tutor*, *role*, the plugin will insert role_assignment records for that tutor on the student's context, in the given role.

Item	Result
Version	2019071201
Release	0.2
Requires	2012061700
Usage	N/A
Author/copyright holder	UCL
Online reviews	N/A
Compatibility	N/A

2 Review Results

2.1 Security

The following potential security issues have been observed:

- `field\profile::get_equivalent_moodle_id()` puts data directly into SQL without using parameters.
- `dataportexternal::get_relationships_in_scope()` does not sanitise field mappings, so if someone with access to change the plugin settings were to enter an SQL injection into the tutor, student or role mappings, they could inject that into the external database query.
- `dataportinternal::get_all_roles()` and `dataportinternal::get_relationships_in_scope()` do not sanitise the `$this->localrolefield` field before putting it into the `get_records()` or `get_records_sql()` call. So if someone with access to change the plugin settings were to enter an SQL injection into the role mappings they could inject that into the Moodle database.

Note: The SQL injections would only be able to run by someone with access to change the plugin settings, so a site admin, however they should still be fixed.

Item	Result
Permissions	OK – Sync is run via scheduled task or CLI script, so no user will be manually running anything. Configuration uses standard Moodle admin settings.
Authentication	OK – As above.
Form inputs	OK – Configuration uses standard Moodle settings form.

Item	Result
Other inputs	NOT OK – Several instances of data being inserted into SQL without sanitisation, leading to SQL injection potential, if plugin configuration settings altered maliciously.
External data in HTML	OK
Cross site scripting	OK
SQL parametrised	NOT OK – Some SQL queries on both external and internal moodle database are open to SQL injections, if plugin configuration settings altered maliciously.
Data exposure	OK
Shell commands	OK
CSRF	OK
Data leakage	No data leakage observed.
Transmission to third parties	N/A

2.2 Coding Quality

Coding quality is acceptable, however, as outlined in the Security section, there are several SQL injection possibilities which need to be fixed.

Item	Result
Outstanding bugs upstream	0
Installation	OK
Notices seen	OK
Basic functionality	OK - Basic sync functionality works to create role_assignments.
Admin functionality	OK - Configuration form works.
Backup	N/A
Restored	N/A
Removed	OK
Coding standards violations	A TOTAL OF 172 ERRORS AND 26 WARNINGS WERE FOUND IN 9 FILES
Abstraction	OK – Plugin uses classes and interfaces. Method length is okay.
Unit testing	Not checked

Item	Result
Side effects	OK - No side effects observed.
Code documentation	OK – Code documentation is acceptable.

2.3 Performance

No performance issues observed.

Item	Result
Really big synchronous jobs	OK
Database killing queries	OK
Page response time	OK
Disk usage	OK

3 Review Environment

Item	Result
Plugin name	enrol_dbuserrel
Plugin git hash	059402e281a0d179c26dba2cafb9667f79ed8ea1
Plugin upstream repository	https://github.com/uclmoodle/moodle-enrol_dbuserrel/
Plugin repository	ssh://reviews.ci.catalyst-eu.net:29418/moodle-enrol_dbuserrel
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