chamilo / **chamilo-lms** Public

Code | Issues 399 | Pull requests 13 | Discussions | Actions | Projects

Commit `2a9f060`

AngelFQC committed 3 weeks ago Verified

```
Security: Add CourseRelUserStateProcessor and improve course catalog filtering logic

See advisory GHSA-x373-8j9j-g5pj
```

master · v2.0.0 v2.0.0-RC.3

1 parent 3608d76 commit 2a9f060

3 files changed +55 -3 lines changed

Top

Filter files…

- config
  - services.yaml
- src/CoreBundle
  - Entity
    - CourseRelUser.php
  - Helpers
    - CourseCatalogueHelper.php

3 files changed +55 -3 lines changed

Search within code

config/services.yaml

```
@@ -126,6 +126,10 @@ services:
126 126         bind:
127 127           $persistProcessor: '@api_platform.doctrine.orm.state.persist_processor'
128 128
+ 129     Chamilo\CoreBundle\State\CourseRelUserStateProcessor:
+ 130       bind:
```

```
131 +         $persistProcessor: '@api_platform.doctrine.orm.state.persist_processor'
132 +
129 133       Chamilo\CoreBundle\State\UserRelUserStateProcessor:
130 134         bind:
131 135           $persistProcessor: '@api_platform.doctrine.orm.state.persist_processor'
```

src/CoreBundle/Entity/CourseRelUser.php

```
@@ -16,6 +16,7 @@
16 16  use ApiPlatform\Metadata\Post;
17 17  use Chamilo\CoreBundle\Filter\PartialSearchOrFilter;
18 18  use Chamilo\CoreBundle\Repository\CourseRelUserRepository;
   19 + use Chamilo\CoreBundle\State\CourseRelUserStateProcessor;
19 20  use Chamilo\CoreBundle\State\UserCourseSubscriptionsStateProvider;
20 21  use Chamilo\CoreBundle\Traits\UserTrait;
21 22  use Doctrine\ORM\Mapping as ORM;
@@ -29,9 +30,13 @@
29 30   */
30 31  #[ApiResource(
31 32      operations: [
32    -         new Get(security: "is_granted('ROLE_ADMIN') or object.user == user"),
33    -         new GetCollection(security: "is_granted('ROLE_ADMIN')"),
34    -         new Post(security: "is_granted('ROLE_ADMIN') or is_granted('ROLE_USER')"),
   33 +         new Get(security: "is_granted('ROLE_ADMIN') or is_granted('ROLE_TEACHER') or is_granted('ROLE_SESSION_MANAGER') or object.user == user"),
   34 +         new GetCollection(security: "is_granted('ROLE_ADMIN') or is_granted('VIEW', object.course)"),
   35 +         new Post(
   36 +             security: "is_granted('ROLE_USER')",
   37 +             securityPostDenormalize: "object.getUser() == user",
   38 +             processor: CourseRelUserStateProcessor::class
   39 +         ),
35 40           new GetCollection(
36 41               uriTemplate: '/me/courses.{_format}',
37 42               paginationEnabled: true,
```

...oreBundle/Helpers/CourseCatalogueHelper.php

```
@@ -15,6 +15,8 @@
15 15  use Chamilo\CoreBundle\Settings\SettingsManager;
16 16  use Doctrine\ORM\EntityManagerInterface;
17 17  use Doctrine\ORM\EntityRepository;
   18 + use Doctrine\ORM\NonUniqueResultException;
   19 + use Doctrine\ORM\NoResultException;
18 20  use Doctrine\ORM\Query\Expr\Join;
19 21  use Doctrine\ORM\QueryBuilder;
20 22
@@ -181,6 +183,47 @@ public function
    addOnlySelectedCategoriesCondition(QueryBuilder $qb): void
181 183          ;
182 184      }
183 185
   186 +    /**
   187 +     * Returns true if the given course passes all catalogue filters
       (visibility, show-in-catalogue,
   188 +     * avoided-courses, selected-categories) that the public catalogue endpoint
       applies.
   189 +     */
   190 +    public function isCourseInPublicCatalogue(Course $course): bool
   191 +    {
   192 +        $courseRepo = $this->entityManager->getRepository(Course::class);
   193 +        $qb = $courseRepo->createQueryBuilder('c');
   194 +
   195 +        $qb
   196 +            ->select('COUNT(c.id)')
   197 +            ->andWhere('c.id = :courseId')
   198 +            ->setParameter('courseId', $course->getId())
   199 +        ;
   200 +
   201 +        if ($this->accessUrlHelper->isMultiple()) {
   202 +            $qb
   203 +                ->innerJoin(
   204 +                    'c.urls',
   205 +                    'aurc',
   206 +                    Join::WITH,
   207 +                    $qb->expr()->eq('aurc.url', ':accessUrl')
```

```
208 + )
209 + ->setParameter('accessUrl', $this->accessUrlHelper->getCurrent()->getId())
210 + ;
211 + }
212 +
213 + $this->addAvoidedCoursesCondition($qb);
214 + $this->addOnlySelectedCategoriesCondition($qb);
215 + $this->addShowInCatalogueCondition($qb);
216 + $this->addVisibilityCondition($qb, true);
217 +
218 + try {
219 + return (int) $qb->getQuery()->getSingleScalarResult() > 0;
220 + } catch (NoResultException) {
221 + return false;
222 + } catch (NonUniqueResultException) {
223 + return true;
224 + }
225 + }
226 +
184 227 public function addAvoidedCoursesCondition(QueryBuilder $qb): void
185 228 {
186 229 $isStudent = (bool) $this->userHelper->getCurrent()?->isStudent();
```

Comments 0

Please sign in to comment.