Users with ROLE_COURSE_ADMIN can create new users

Moderate lkiesow published GHSA-94qw-r73x-j7hg on Jan 29, 2020

Package

No package listed

Affected versions	Patched versions
< 7.6, 8.0	7.6, 8.1

Description

Impact

Users with the role `ROLE_COURSE_ADMIN` can use the user-utils endpoint to create new users not including the role `ROLE_ADMIN`. For example:

```
# Use the admin to create a new user with ROLE_COURSE_ADMIN using the admin user.
# We expect this to work.
% curl -i -u admin:opencast 'https://example.opencast.org/user-utils/xy.json' -X PUT \
  --data 'password=f&roles=%5B%22ROLE_COURSE_ADMIN%22%5D'
HTTP/2 201

# Use the new user to create more new users.
# We don't expüect a user with just role ROLE_COURSE_ADMIN to succeed.
# But it does work
% curl -i -u xy:f 'https://example.opencast.org/user-utils/ab.json' -X PUT \
  --data 'password=f&roles=%5B%22ROLE_COURSE_ADMIN%22%5D'
HTTP/2 201
```

`ROLE_COURSE_ADMIN` is a non-standard role in Opencast which is referenced neither in the documentation nor in any code (except for tests) but only in the security configuration. From the name – implying an admin for a specific course – users would never expect that this role allows user creation.

Patches

This issue is fixed in 7.6 and 8.1 which both ship a new default security configuration.

Workarounds

You can fix this issue by removing all instances of `ROLE_COURSE_ADMIN` in your organization's security configuration (`etc/security/mh_default_org.xml` by default).

For more information

If you have any questions or comments about this advisory:

- Open an issue in opencast/opencast
- For security-relevant information, email us at security@opencast.org

Severity

Moderate

CVE ID

CVE-2020-5231

Weaknesses

No CWEs