Bug 2446963 (CVE-2026-32589) - CVE-2026-32589 mirror-registry: quay: insecure direct object reference in BlobUpload

Keywords: Security

Status: NEW

Alias: CVE-2026-32589

Deadline: 2026-04-15

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-03-12 15:01 UTC by OSIDB Bzimport

Modified: 2026-04-08 16:55 UTC (History)

CC List: 4 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-03-12 15:01:16 UTC Description

```
Red Hat Quay contains an Insecure Direct Object Reference
(IDOR) vulnerability in the OCI blob upload protocol. Any
authenticated user with push access to any repository can
perform unauthorized read, write, and delete operations
against in-progress blob uploads belonging to other tenants,
without holding any permissions on those tenants'
repositories.

Requirements to exploit: Attacker needs to be logged into the
web app / initiate curl authenticated requests.

Components affected:
```

```
Mirror Registry for OpenShift – BlobUpload functionality /
affected database column sha_state
Quay deployed on OpenShift 4.20 – BlobUpload functionality /
affected database column sha_state

Version affected: latest release
```

Note

You need to log in before you can comment on or make changes to this bug.