Bug 2446964 (CVE-2026-32590) - CVE-2026-32590 mirror-registry: remote code execution using pickle deserialization

Keywords: Security

Status: NEW

Alias: CVE-2026-32590

Deadline: 2026-04-15

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-03-12 15:09 UTC by OSIDB Bzimport

Modified: 2026-04-08 16:58 UTC (History)

CC List: 3 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-03-12 15:09:28 UTC Description

```
A remote code execution (RCE) vulnerability was identified in
Red Hat Quay v3.12.x resulting from the unsafe use of Python's
pickle module to serialize and deserialize hashlib state
objects stored in the database. The affected fields —
sha_state and piece_sha_state on the BlobUpload model — store
the in-progress SHA-256 and SHA-1 hash state for resumable
container image layer uploads.

Requirements to exploit: Attacker needs to be logged into the
web app / initiate podman execution from host.

Component affected:
```

```
Mirror Registry for OpenShift – 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.