Bug 2446965 (CVE-2026-32591) - CVE-2026-32591 mirror-registry: quay: server-side request forgery in proxy cache upstream registry configuration

Keywords: Security

Status: NEW

Alias: CVE-2026-32591

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 15:14 UTC by OSIDB Bzimport

Modified: 2026-04-08 17:03 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 15:14:01 UTC Description

A Server-Side Request Forgery (SSRF) vulnerability was identified in Red Hat Quay v3.12.x within the Proxy Cache configuration feature. An authenticated organization administrator can supply an attacker-controlled hostname as the upstream_registry parameter when creating or validating a proxy cache configuration. Quay instantiates a network connection to the supplied hostname with no validation against internal address ranges, private IP space, or cloud metadata endpoints.

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

```
Component affected:
Mirror Registry for OpenShift – Proxy Cache configuration
feature
Quay deployed on OpenShift 4.20 – Proxy Cache configuration
feature

Version affected: latest releases
```

Note

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