



# Mirror-registry: quay: server-side request forgery in proxy cache upstream registry configuration

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2026-32591
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-08 18:26:00 UTC
<b>Updated</b>	2026-04-08 21:26:13 UTC
<b>Description</b>	A flaw was found in Red Hat Quay's Proxy Cache configuration feature. When an organization administrator configures an

## Risk And Classification

**Primary CVSS:** v3.1 5.2 MEDIUM from secalert@redhat.com

**CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N**

**Problem Types:** CWE-918 | CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	5.2	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N
3.1	CNA	CVSS	5.2	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**High**

User Interaction

**Required**

Scope

**Unchanged**

Confidentiality

**High**

Integrity

**Low**

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Mirror Registry For Red Hat OpenShift	Not specified	Not specified
CNA	Red Hat	Mirror Registry For Red Hat OpenShift 2	Not specified	Not specified
CNA	Red Hat	Red Hat Quay 3	Not specified	Not specified
CNA	Red Hat	Red Hat Quay 3	Not specified	Not specified

### References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-32591	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Red Hat would like to thank Antony Di Scala and Michael Whale for reporting this issue.  
(en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-03-12T15:09:38.210Z	Reported to Red Hat.
CNA	2026-04-08T00:00:00.000Z	Made public.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)