Mirror-registry: quay: insecure direct object reference in blobupload

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-32589
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 18:25:59 UTC
Updated	2026-04-08 21:26:13 UTC
Description	A flaw was found in Red Hat Quay's container image upload process. An authenticated user with push access to any repos

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from secalert@redhat.com

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

Problem Types: CWE-639 | CWE-639 Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
High

Privileges Required
Low

User Interaction
Required

Scope
Changed

Confidentiality
Low

Integrity
High

Availability

Low

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

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
access.redhat.com/security/cve/CVE-2026-32589	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.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	2026-03-12T14:43:07.878Z	Reported to Red Hat.
CNA	2026-04-08T00:00:00.000Z	Made public.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**