CVE-2024-3727

VEX

Public on May 9, 2024

Last modified: September 25, 2025 at 7:52:55 AM UTC

MODERATE

Moderate severity

What does this mean?

8.3

CVSS v3 Score Breakdown

Jump to section

Description

A flaw was found in the github.com/containers/image library. This flaw allows attackers to trigger unexpected authenticated registry accesses on behalf of a victim user, causing resource exhaustion, local path traversal, and other attacks.

Statement

Some conditions are necessary for this attack to occur, such as the attacker being able to upload malicious images to the registry and persuade a victim to pull them. Hence, the severity of this flaw was rated as Moderate.

Additional information

- Bugzilla 2274767: containers/image: digest type does not guarantee valid type
- CWE-354: Improper Validation of Integrity Check Value
- FAQ: Frequently asked questions about CVE-2024-3727

External references

- https://www.cve.org/CVERecord?id=CVE-2024-3727
- https://nvd.nist.gov/vuln/detail/CVE-2024-3727

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	OADP-1.3-RHEL-9
Components	oadp/oadp-velero-plugin-rhel9
State	Fixed
Justification	None
Errata	RHSA-2024:9960
Release Date	November 19, 2024

Products / Services	Red Hat Advanced Cluster Security 4.4
Components	advanced-cluster-security/rhacs-central-db-rhel8
State	Fixed
Justification	None
Errata	RHSA-2024:6054
Release Date	August 29, 2024

Products / Services	Red Hat Advanced Cluster Security 4.4

1-10 of 167

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD

	Red Hat	NVD
CVSS v3 Base Score	8.3	N/A
Attack Vector	Network	N/A
Attack Complexity	High	N/A
Privileges Required	None	N/A
User Interaction	Required	N/A
Scope	Changed	N/A
Confidentiality Impact	High	N/A
Integrity Impact	High	N/A
Availability Impact	High	N/A

CVSS v3 Vector

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

Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors? ›

My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?

What can I do if my product is listed as "Will not fix"?

What can I do if my product is listed as "Fix deferred"?

What is a mitigation?

I have a Red Hat product but it is not in the above list, is it affected?

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

My product is listed as "Out of Support Scope". What does this mean?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: September 25, 2025 at 7:52:55 AM UTC

Related Sites

All systems operational

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie Preferences and Opt-Out Rights