CVE-2025-57854

VEX

Public on April 8, 2026

Last modified: April 8, 2026 at 1:55:01 PM UTC

MODERATE

Moderate severity

What does this mean?

6.4

CVSS v3 Score Breakdown

Jump to section

Description | Statement | Additional information | Affected Packages | CVSS Score Details | Weakness (CWE) | Acknowledgements | FAQ

Description

A container privilege escalation flaw was found in certain OpenShift Update Service (OSUS) images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, may be able to leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.

Statement

Red Hat Product Security has rated this vulnerability as moderate severity for affected pr oducts which run on OpenShift. The vulnerability allows for potential privilege escalation within a container, but OpenShift's default, multi-layered security posture effectively miti gates this risk.

The primary controls include the default Security Context Constraints (SCC), which sever ely limit a container's permissions from the start, and SELinux, which enforces mandatory access control to ensure strict isolation. While other container runtime environments may have different controls available and require case-by-case analysis, OpenShift's built-in d efenses are designed to prevent this type of attack.

Out of Box RHEL configuration isolates a single process inside a container. Unless multiple processes are packaged inside a single container, that defeats the principle behind contai nerization, this bug can not be used to meaningfully escalate privileges.

Also, RHEL, and any common linux distributions do NOT add any additional users to the ro ot group. The presence of the root group is strictly due to conformance with POSIX permi ssion management requirements and can be considered to be an artifact of filesystem per mission limitations.

Additional information

- Bugzilla 2391107: osus-operator: privilege escalation via excessive /etc/passwd permissions
- CWE-276: Incorrect Default Permissions

External references

- https://www.cve.org/CVERecord?id=CVE-2025-57854
- https://nvd.nist.gov/vuln/detail/CVE-2025-57854

Affected Packages and Issued Red Hat Security Errata

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.

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat OpenShift Update Service
Components	openshift-update-service/openshift-update-service-rhel8-operator
State	Affected
Justification	None
Errata	
Release Date	

1 of 1

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).

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	6.4	N/A	N/A
Attack Vector	Local	N/A	N/A
Attack Complexity	High	N/A	N/A
Privileges Required	High	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Unchanged	N/A	N/A
Confidentiality Impact	High	N/A	N/A
Integrity Impact	High	N/A	N/A
Availability Impact	High	N/A	N/A

CVSS v3 Vector

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

Acknowledgements

Red Hat would like to thank Antony Di Scala and Michael Whale for reporting this issue.

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?**

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: April 8, 2026 at 1:55:01 PM UTC