



## Bug 2391099 (CVE-2025-57848) - CVE-2025-57848 container-native-virtualization: privilege escalation via excessive /etc/passwd permissions

**Keywords:** Security ✕ ▼

**Reported:** 2025-08-26 18:29 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2025-10-23 20:05 UTC ([History](#))

**Alias:** CVE-2025-57848

**CC List:** 6 users ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:**

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

**Attachments** ([Terms of Use](#))

OSIDB Bzimport 2025-08-26 18:29:41 UTC

[Description](#)

```
The /etc/passwd file is created during build time with group-writable permissions. 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.
```

Note

You need to [log in](#) before you can comment on or make changes to this bug.

