



Bug 2394418 (CVE-2025-58712) - CVE-2025-58712 amq: privilege escalation via excessive /etc/passwd permissions

Keywords: Security ✕

Reported: 2025-09-10 17:32 UTC by OSIDB Bzimport

Status: NEW

Modified: 2025-10-22 18:14 UTC ([History](#))

Alias: CVE-2025-58712

CC List: 5 users ([show](#))

Deadline: 2025-10-07

Fixed In Version:

Product: Security Response

Clone Of:

Component: vulnerability

Environment:

Last Closed:

Embargoed:

Version: unspecified

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 [\(Terms of Use\)](#)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2025:17562	0	None	None	None	2025-10-08 14:39:28 UTC

OSIDB Bzimport 2025-09-10 17:32:33 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.

errata-xmlrpc 2025-10-08 14:39:27 UTC

[Comment 3](#)

This issue has been addressed in the following products:

RHEL-9 based Middleware Containers

Via RHSA-2025:17562 <https://access.redhat.com/errata/RHSA-2025:17562>

Note

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

