Bug 2391103 (CVE-2025-57850) - CVE-2025-57850 codeready-ws: privilege escalation via excessive /etc/passwd permissions

Keywords: Security

Status: NEW

Alias: CVE-2025-57850

Deadline: 2025-12-02

Product: Security Response

Component: vulnerability

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

Reported: 2025-08-26 18:44 UTC by OSIDB Bzimport

Modified: 2025-12-02 15:51 UTC (History)

CC List: 2 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2025-08-26 18:44:24 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.