podman kube play symlink traversal vulnerability

High **Luap99** published **GHSA-wp3j-xq48-xpjw** on Sep 4, 2025

Package

github.com/containers/podman (Go)

Affected versions

v4.0.0 to v5.6.0

Patched versions

v5.6.1

Description

Impact

The podman kube play command can overwrite host files when the kube file contains a ConfigMap or Secret volume mount and the volume already contains a symlink to a host file.
This allows a malicious container to write to arbitrary files on the host BUT the attacker only controls the target path not the contents that will be written to the file. The contents are defined in the yaml file by the end user.

Requirements to exploit:

podman kube play must be used with a ConfigMap or Secret volume mount AND must be run more than once on the same volume. All the attacker has to do is create the malicious symlink on the volume the first time it is started. After that all following starts would follow the symlink and write to the host location.

Patches

Fixed in podman v5.6.1
`43fbde4`

Workarounds

Don't use podman kube play with ConfigMap or Secret volume mounts.

PR with test for CI

Adding on 9/8/2025 by **@TomSweeneyRedHat** , this is the PR containing the test in CI: #27001

Severity

High 8.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2025-9566

Weaknesses

No CWEs

Credits

Luap99 Reporter