What is a host-path mount?

A host-path mount maps a directory or file from the host into a container (Docker `-v /host/path:/in/container`, Kubernetes `hostPath` volume). It is useful for sharing data, but mounting a sensitive path lets a compromised container read host secrets or write to host-controlled locations and escape to the node. Mounting `/`, `/etc`, `/var/run/docker.sock`, or a writable system directory effectively breaks isolation. Prefer named volumes and, in Kubernetes, block hostPath with policy.

HOW IT WORKS

01 The abuse and payload

A dangerous mount turns a container compromise into a host compromise:

- Mounting host root or `/etc`: read `/etc/shadow`, SSH keys, or cloud credentials; with write access, add a root user or a cron job on the host.
- Mounting a writable system path (for example a host `bin` or a kubelet directory): drop a binary the host will execute.
- Mounting `/var/run/docker.sock`: full daemon control (see the Docker socket).
- Writing to `/host/etc/cron.d/` to get root code execution on the node.

Documented techniques shown for defenders.

> AS POWERFUL AS THE PATH
>
> *A host-path mount is exactly as dangerous as what it exposes. Mounting `/`, `/etc`, system directories, or the Docker socket hands a compromised container a direct route to the node.*

HOW TO DEFEND

- Avoid hostPath for application workloads. Use named volumes, CSI drivers, or cloud storage instead.
- Never mount sensitive host paths (`/`, `/etc`, `/var/run`, system binaries) into containers.
- Mount read-only when a mount is unavoidable, and scope it to the narrowest possible directory.
- In Kubernetes, block hostPath with Pod Security Standards and admission control (or allow-list specific safe paths).
- Scan manifests for hostPath volumes and risky `-v` mounts.

SOURCES

[1] Kubernetes docs: Volumes (hostPath)

[2] NIST SP 800-190 Application Container Security Guide

[3] MITRE ATT&CK: Containers Matrix

Find the container escape paths before an attacker does.

`securelayer7.net/learn/containers/what-is-a-host-path-mount`

Open online