Writable hostPath mount

hostPath volume mounts a directory or a file from the host to the container. Attackers who have permissions to create a new container in the cluster may create one with a writable hostPath volume and gain persistence on the underlying host. For example, the latter can be achieved by creating a cron job on the host.

Info

ID: MS-TA9013
Tactic: Persistence, Privilege Escalation, Lateral Movement
MITRE technique: T1611

Mitigations

ID	Mitigation	Description
MS-M9013	Restrict over permissive containers	Block sensitive volume mounts using admission controller.
MS-M9016	Restrict File and Directory Permissions	Use read-only volumes.
MS-M9011	Restrict Container Runtime using LSM	Use AppArmor to restrict file writing.
MS-M9017	Ensure that pods meet defined Pod Security Standards	Use `Baseline` or `Restricted` pod security standards to prevent exploiting writable hostPath mount.