Privileged container

A privileged container is a container that has all the capabilities of the host machine, which lifts all the limitations regular containers have. Practically, this means that privileged containers can do almost every action that can be performed directly on the host. Attackers who gain access to a privileged container, or have permissions to create a new privileged container (by using the compromised pod's service account, for example), can get access to the host's resources.

Info

ID: MS-TA9018
Tactic: Privilege Escalation
MITRE technique: T1610

Mitigations

ID	Mitigation	Description
MS-M9013	Restrict over permissive containers	Block privileged containers using admission controller.
MS-M9017	Ensure that pods meet defined Pod Security Standards	Restrict privileged containers using pod security standards.
MS-M9005.003	Gate images deployed to Kubernetes cluster	Restrict deployment of new containers from trusted supply chain