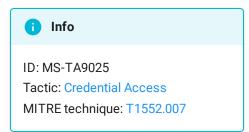**Threat Matrix for Kubernetes**

List Kubernetes secrets

A Kubernetes secret is an object that lets users store and manage sensitive information, such as passwords and connection strings in the cluster. Secrets can be consumed by reference in the pod configuration. Attackers who have permissions to retrieve the secrets from the API server (by using the pod service account, for example) can access sensitive information that might include credentials to various services.

> **Info**
>
> ID: MS-TA9025
> Tactic: Credential Access
> MITRE technique: T1552.007

Mitigations

ID	Mitigation	Description
MS-M9003	Adhere to least-privilege principle	Limit users and service accounts access to Kubernetes secrets.
MS-M9022	Use Managed Secret Store	Use cloud provider secret store to securely manage credentials in the cluster
MS-M9023	Remove unused secrets objects from the cluster	Remove unused secrets from the cluster.
MS-M9024	Restrict access to etcd	Restrict access to etcd.

Made with Material for MkDocs