What is SelfSubjectRulesReview abuse?

SelfSubjectRulesReview is a Kubernetes API that returns the exact set of actions the calling identity can perform in a namespace. After stealing a token or impersonating an identity, an attacker calls it to map their capabilities instantly, skipping noisy trial and error. It is available to all authenticated users by design, so the defence is least-privilege identities and detection of post-compromise recon, not disabling the API.

HOW IT WORKS

01 How it works and example

Having compromised a token or impersonated an identity, the attacker calls SelfSubjectRulesReview and immediately learns which verbs and resources are in reach, so they target only actions that will succeed. In a 2026 cluster intrusion this capability mapping let the agent move straight to useful actions without tripping the alarms that failed attempts would raise.

SOURCES

[1] MITRE ATT&CK Cloud Matrix

[2] HuggingFace, Agent intrusion technical timeline

[3] Kubernetes authorization: checking API access

Find the cloud and Kubernetes attack paths before someone else does.

securelayer7.net/learn/cloud-security/selfsubjectrulesreview-abuse

Open online