What is Kubernetes TokenRequest abuse?

The Kubernetes TokenRequest API mints short-lived, scoped service-account tokens on demand. An attacker who compromises a pod or identity that can call it can request fresh tokens for other service accounts, for example a CSI driver, extending access and evading detection that watches for static, long-lived tokens. Defend by scoping TokenRequest permissions tightly and monitoring token minting.

HOW IT WORKS

01 How it works and example

An attacker who takes over a pod identity that can call TokenRequest, such as a CSI driver pod, uses it to mint fresh tokens for privileged service accounts. The new tokens are valid and short-lived, so credential-theft detection tuned for static secrets does not flag them, and the attacker refreshes access as needed. This was part of a 2026 machine-speed Kubernetes intrusion.

SOURCES

[1] MITRE ATT&CK Cloud Matrix

[2] HuggingFace, Agent intrusion technical timeline

[3] Kubernetes TokenRequest API

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

securelayer7.net/learn/cloud-security/kubernetes-tokenrequest-abuse

Open online