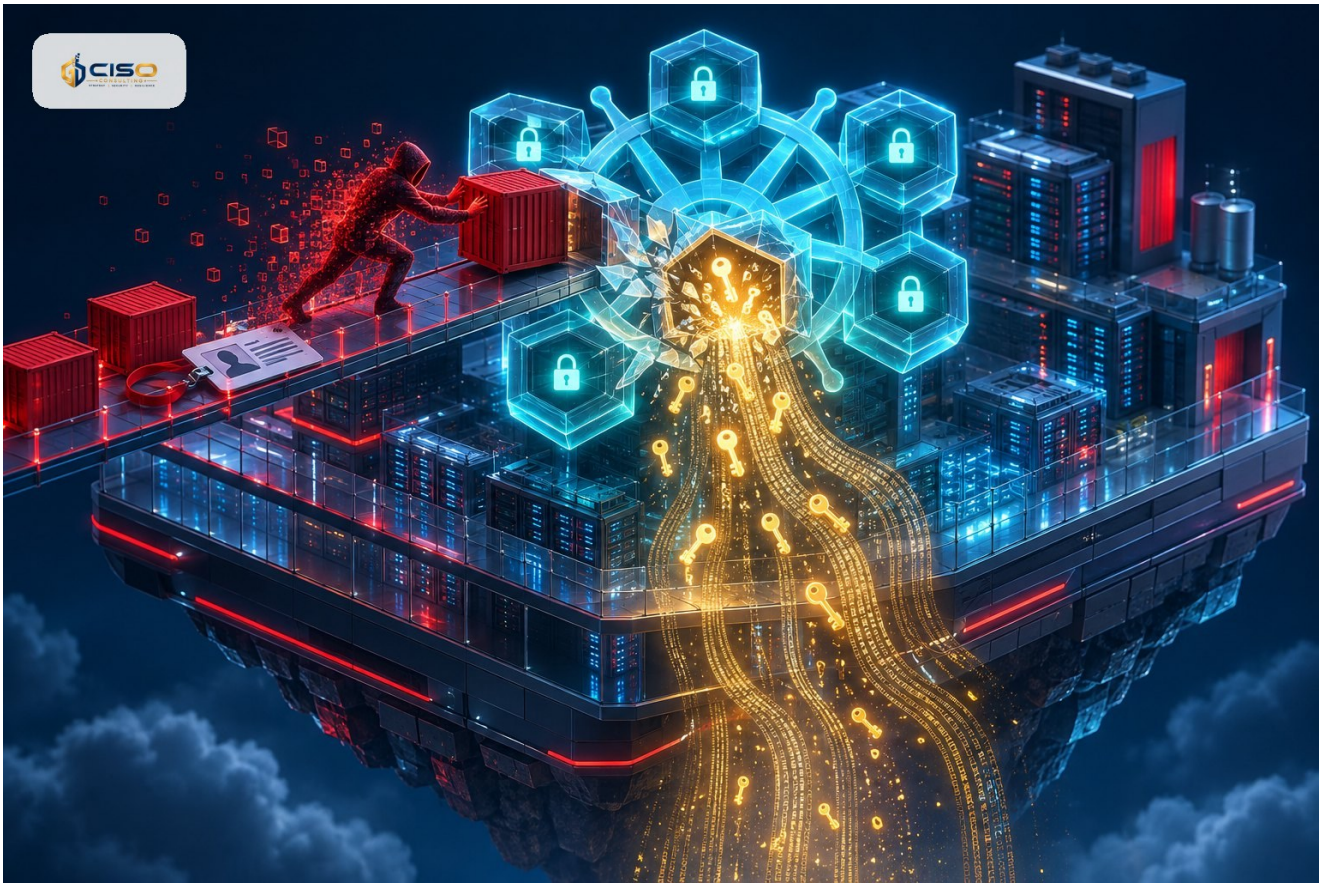
Rackspace Spot breach exposed Kubernetes secrets in customer clusters



Rackspace told customers that attackers used compromised credentials to breach its Rackspace Spot cloud platform, deploy unauthorized workloads and access Kubernetes secrets in customer clusters.

- Rackspace notified customers of a breach of its Rackspace Spot cloud platform.
- The attackers reportedly gained entry using compromised credentials.
- They were able to deploy unauthorized workloads.
- They could also access Kubernetes secrets in customer clusters.
- The source excerpt gives no further detail on scope, timing or number of affected customers.

Rackspace has warned customers that its Rackspace Spot cloud platform was breached. According to the notice described by BleepingComputer, attackers used compromised credentials to get in.

What the attackers could do

Once inside, the attackers were able to deploy unauthorized workloads and to access **Kubernetes secrets** in customer clusters. Secrets in Kubernetes typically hold items such as credentials, tokens and keys, so access to them can extend the impact beyond the platform itself to systems those secrets protect.

The source excerpt available to us does not state how many customers were affected, when the activity took place, or what Rackspace has done to contain it. We have not filled those gaps and recommend reading Rackspace's customer notice directly.

What this means for regulated institutions

Institutions that use Rackspace Spot, or hold workloads with any provider where credentials could be compromised, should treat this as a prompt to check their own exposure. The practical priority is to establish whether any of your clusters were affected, and to assume that secrets stored in an affected cluster may need to be replaced.

This is also a reminder that third-party cloud incidents can trigger your own obligations for assessment, escalation and, where relevant, notification under the frameworks that apply to your organization.

What to do now

1. Check whether your organization has any clusters or accounts on Rackspace Spot and read the Rackspace customer notice.
2. If you are affected, rotate all Kubernetes secrets, tokens and credentials stored in those clusters.
3. Review clusters for unexpected or unauthorized workloads and for unusual access activity.
4. Rotate and enforce MFA where possible on cloud platform accounts and credentials used to manage clusters.
5. Record the event under your third-party and incident processes, and assess any reporting duties to your regulator.