Rackspace to close Spot cloud platform after breach exposed Kubernetes secrets



Rackspace will discontinue its Spot Kubernetes platform on 8 December 2026 after an intrusion using compromised credentials. Customers must migrate, rotate credentials and review logs.

- Attackers entered Rackspace Spot on 17 November using compromised credentials and were detected on 18 November after a customer report.
- They could create pods in customer clusters, read Kubernetes Secrets, and list nodes and volumes.
- Rackspace says the Spot environment is segmented and it has found no evidence of access to core systems or other customers' environments.
- The service ends on 8 December 2026 at 5 PM Central Time, after which workloads are terminated and data is inaccessible.
- All Spot customers should treat API tokens, refresh tokens, kubeconfigs and Secrets as potentially

> compromised.

Rackspace has told customers it will wind down Rackspace Spot, its platform for running containerised applications on Kubernetes, following a security breach. Customers have until 8 December 2026, 5 PM Central Time, to download data and move workloads. After that, remaining workloads will be terminated and data will no longer be accessible.

What happened

According to the notification reported by BleepingComputer, attackers used compromised credentials to access Spot on 17 November. They were able to create unauthorised pods in customer Kubernetes clusters, read Kubernetes Secrets, and list nodes and volumes. Rackspace found the intrusion on 18 November after a customer report, disabled access to the administration console, and restored service on 21 November after an extended outage.

Rackspace states that the Spot environment is segmented from its core infrastructure and that it has found no evidence of unauthorised access to core systems or to other Rackspace customers' environments. It has not said whether it will extend the deadline or reconsider the closure.

What Spot customers should do

Rackspace asks all Spot customers to treat API tokens, refresh tokens, kubeconfigs and Kubernetes Secrets as potentially compromised, whether or not they received an earlier breach notice. It also recommends reviewing access logs back to 16 November and looking for suspicious Kubernetes objects. The indicators it published are the IP address 23.224.79.106, the range 23.224.0.0/15, and pod or object names starting with i1, glm- or probe.

For institutions in the Kingdom, the closure adds a forced migration to an incident response task, so both should be handled together and documented.

What to do now

1. Confirm whether any workload or business unit uses Rackspace Spot, including teams outside central IT.
2. Rotate all API tokens, refresh tokens, kubeconfigs and Kubernetes Secrets, and any downstream credentials stored in them.
3. Search access logs from 16 November for the published IP address, range and the i1, glm- and probe object prefixes.
4. Plan migration and data export well before 8 December 2026, with a fallback if the deadline holds.
5. Record the incident and the exit in your third-party and incident registers, and assess whether regulator or PDPL notification duties apply if personal data was in affected clusters.