Rackspace تُغلق منصة Spot السحابية بعد اختراق طال أسرار Kubernetes



ستوقف Rackspace منصة Spot في 8 ديسمبر 2026 بعد اختراق عبر بيانات اعتماد مسروقة. على العملاء نقل أعباء العمل وتدوير بيانات الاعتماد ومراجعة السجلات.

- دخل المهاجمون منصة Rackspace Spot في 17 نوفمبر ببيانات اعتماد مخترقة، واكتُشف الاختراق في 18 نوفمبر بعد بلاغ من أحد العملاء.
- أتاح الاختراق إنشاء pods في مجموعات العملاء وقراءة Kubernetes Secrets وسرد العُقد والأقراص.
- تقول Rackspace إن بيئة Spot معزولة ولم تجد دليلًا على وصول إلى أنظمتها الأساسية أو بيئات عملاء آخرين.
- تنتهي الخدمة في 8 ديسمبر 2026 الساعة 5 مساءً بتوقيت وسط الولايات المتحدة، وبعدها تُنهى الأعباء وتصبح البيانات غير متاحة.

- على جميع عملاء Spot اعتبار رموز API ورموز التحديث وملفات kubeconfig وSecrets مُعرَّضة للاختراق.

أبلغت Rackspace عملاءها بأنها ستُنهي خدمة Rackspace Spot، وهي منصة لتشغيل التطبيقات المحوّلة إلى حاويات على Kubernetes، وذلك بعد اختراق أمني. أمام العملاء مهلة حتى 8 ديسمبر 2026 الساعة 5 مساءً بتوقيت وسط الولايات المتحدة لتنزيل بياناتهم ونقل أعباء العمل. بعد ذلك تُنهى الأعباء المتبقية ولا تعود البيانات متاحة.

ما الذي حدث

وفق الإشعار الذي نقلته BleepingComputer، استخدم المهاجمون بيانات اعتماد مخترقة للدخول إلى Spot في 17 نوفمبر. تمكنوا من إنشاء pods غير مصرّح بها في مجموعات Kubernetes الخاصة بالعملاء، وقراءة Secrets، وسرد العُقد والأقراص. اكتشفت Rackspace الاختراق في 18 نوفمبر بعد بلاغ من أحد العملاء، وعطّلت الوصول إلى وحدة الإدارة، ثم أعادت الخدمة في 21 نوفمبر بعد انقطاع طويل.

وتذكر Rackspace أن بيئة Spot معزولة عن بنيتها الأساسية، وأنها لم تجد دليلًا على وصول غير مصرّح به إلى أنظمتها الأساسية أو بيئات عملاء آخرين. ولم تُوضح إن كانت ستمدد المهلة أو تعيد النظر في الإغلاق.

ما المطلوب من عملاء Spot

تطلب Rackspace من جميع العملاء اعتبار رموز API ورموز التحديث وملفات kubeconfig وKubernetes Secrets مُعرَّضة للاختراق، سواء تلقّوا إشعاراً سابقاً أم لا. كما توصي بمراجعة سجلات الوصول منذ 16 نوفمبر والبحث عن كائنات Kubernetes مشبوهة. المؤشرات المنشورة هي عنوان IP: 23.224.79.106 والنطاق 23.224.0.0/15 وأسماء pods أو كائنات تبدأ بـ i1 أو glm- أو probe.

وبالنسبة للجهات في المملكة، يضيف الإغلاق نقلًا اضطرارياً إلى مهمة الاستجابة للحادث، ولذلك ينبغي التعامل معهما معاً وتوثيقهما.

ما يجب فعله الآن

1. تحققوا مما إذا كانت أي أعباء عمل أو وحدات أعمال تستخدم Rackspace Spot، بما في ذلك الفرق خارج تقنية المعلومات المركزية.
2. دوّروا جميع رموز API ورموز التحديث وملفات kubeconfig وKubernetes Secrets، وكذلك بيانات الاعتماد اللاحقة المخزنة فيها.
3. ابحثوا في سجلات الوصول منذ 16 نوفمبر عن عنوان IP والنطاق المنشورين وعن بادئات الكائنات i1 وglm- وprobe.
4. خططوا للنقل وتصدير البيانات قبل 8 ديسمبر 2026 بوقت كافٍ، مع خطة بديلة إذا لم تُمدد المهلة.
5. وثّقوا الحادث والخروج من الخدمة في سجلات الأطراف الثالثة والحوادث، وقيّموا التزامات الإبلاغ للجهات التنظيمية ونظام حماية البيانات الشخصية إذا وُجدت بيانات شخصية في المجموعات المتأثرة.