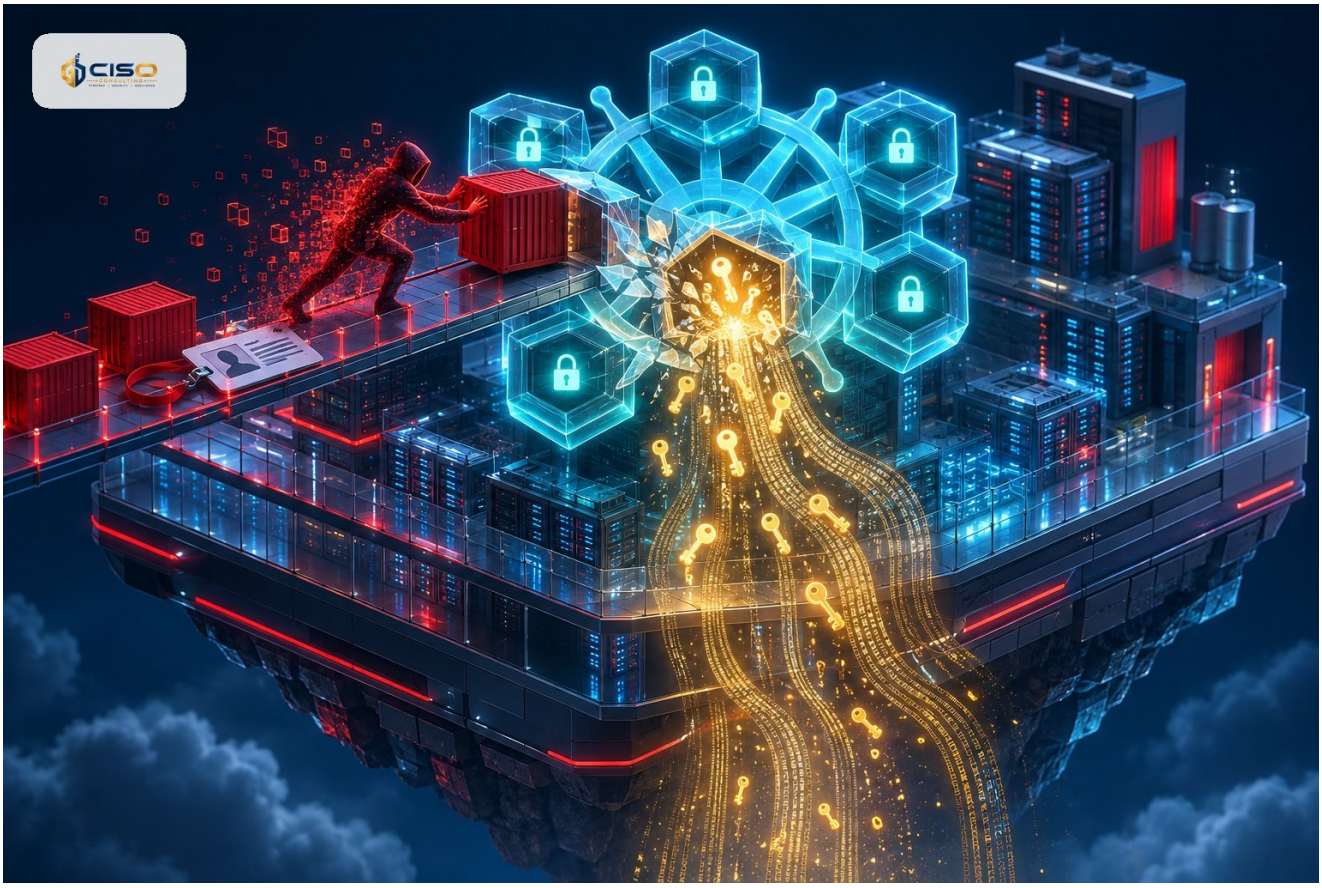
اختراق منصة Rackspace Spot يتيح الوصول إلى أسرار Kubernetes في عناقيد العملاء



أبلغت Rackspace عملاءها بأن مهاجمين استخدموا بيانات اعتماد مخترقة للدخول إلى منصة Rackspace Spot، ونشروا أحمال عمل غير مصرح بها، وتمكنوا من الوصول إلى أسرار Kubernetes في عناقيد العملاء.

- أخطرت Rackspace عملاءها باختراق منصتها السحابية Rackspace Spot.
- دخل المهاجمون إلى المنصة باستخدام بيانات اعتماد مخترقة.
- تمكنوا من نشر أحمال عمل غير مصرح بها.
- كما تمكنوا من الوصول إلى أسرار Kubernetes في عناقيد العملاء.
- لا يتضمن المقتطف المتاح تفاصيل إضافية عن النطاق أو التوقيت أو عدد العملاء المتأثرين.

حذّرت Rackspace عملاءها من اختراق منصتها السحابية Rackspace Spot. وبحسب ما نقله موقع BleepingComputer عن الإشعار، استخدم المهاجمون بيانات اعتماد مخترقة للدخول إلى المنصة.

ما الذي استطاع المهاجمون فعله

بعد الدخول، تمكن المهاجمون من نشر أحمال عمل غير مصرح بها، ومن الوصول إلى **أسرار Kubernetes** في عناقيد العملاء. وتحتوي هذه الأسرار عادةً على بيانات اعتماد ورموز ومفاتيح، ما يعني أن الوصول إليها قد يمتد أثره إلى أنظمة أخرى تحميها هذه الأسرار، لا إلى المنصة وحدها.

لا يوضح المقتطف المتاح لنا عدد العملاء المتأثرين، ولا توقيت النشاط، ولا الإجراءات التي اتخذتها Rackspace للاحتواء. ولم نُكمل هذه النقاط بافتراضات، وننصح بالرجوع إلى إشعار Rackspace للعملاء مباشرة.

الأثر على الجهات المنظّمة

على الجهات التي تستخدم Rackspace Spot، أو تستضيف أحمالًا لدى أي مزود قد تتعرض بيانات اعتماده للاختراق، أن تعتبر ذلك دافعاً لمراجعة تعرضها. والأولوية العملية هي التأكد مما إذا كانت أي من عناقيدها قد تأثرت، وافتراض أن الأسرار المخزنة في أي عنقود متأثر قد تحتاج إلى استبدال.

كما يذكّر الحادث بأن حوادث مزودي الخدمات السحابية من الأطراف الثالثة قد تستوجب على الجهة التقييم والتصعيد، وعند الاقتضاء الإبلاغ، وفق الأطر التي تنطبق عليها.

ما يجب فعله الآن

1. تحقق مما إذا كانت لدى جهتكم عناقيد أو حسابات على Rackspace Spot، واطلعوا على إشعار Rackspace للعملاء.
2. في حال التأثر، قوموا بتدوير جميع أسرار Kubernetes والرموز وبيانات الاعتماد المخزنة في تلك العناقيد.
3. راجعوا العناقيد بحثاً عن أحمال عمل غير متوقعة أو غير مصرح بها وعن نشاط وصول غير معتاد.
4. دوّروا بيانات اعتماد حسابات المنصة السحابية المستخدمة في إدارة العناقيد، وفعّلوا المصادقة متعددة العوامل حيثما أمكن.
5. وثّقوا الحدث ضمن إجراءات الأطراف الثالثة والحوادث، وقيّموا أي التزامات إبلاغ تجاه الجهة المنظِّمة.