

استبدال خمسة إصدارات من أداة OVHcloud CLI على GitHub بنسخة تسرق الأسرار



في 19 أكتوبر استخدم مهاجم حساب مساهم مخترقًا لاستبدال ملفات خمسة إصدارات من أداة OVHcloud CLI على GitHub بنسخة تسرق الأسرار من القرص، وبقيت متاحة حتى 94 دقيقة.

- سيطر المهاجم على حساب مساهم في GitHub واستبدل ملفات التنزيل لخمس إصدارات قائمة من أداة OVHcloud CLI.
- النسخة البديلة مصممة لسرقة الأسرار المخزنة على قرص أي جهاز يشغلها.
- كانت الملفات الخبيثة متاحة من 12:47 إلى 14:21 بتوقيت UTC يوم الاثنين 19 أكتوبر، أي حتى 94 دقيقة.
- التفاصيل مصدرها رواية OVHcloud كما نقلها موقع The Hacker News.

ما الذي حدث

وفق ما أفادت به OVHcloud ونقله موقع The Hacker News، سيطر مهاجم على حساب أحد المساهمين في GitHub يوم الاثنين 19 أكتوبر. ولم ينشر المهاجم إصدارًا جديدًا، بل استبدل ملفات التنزيل المرفقة بخمسة إصدارات قائمة من أداة سطر الأوامر الخاصة بـ OVHcloud.

وكانت الملفات البديلة نسخة مصممة لسرقة الأسرار المخزنة على قرص أي جهاز يشغلها. وبقيت متاحة على GitHub حتى 94 دقيقة، بين 12:47 و14:21 بتوقيت UTC.

لماذا يهم ذلك

لأن ملفات إصدارات قائمة هي التي عُذلت، لم يعد رقم الإصدار المؤلف دليلًا على سلامة الملف المنزّل. وغالبًا ما تعمل أدوات سطر الأوامر هذه على أجهزة مديري الأنظمة وخوادم البناء، حيث تُخزن عادةً بيانات الاعتماد والرموز والمفاتيح. ولا يذكر المصدر عدد من نزلوا الملفات ولا ما إذا كانت أسرار قد سُرقت فعليًا.

الخطوات التالية

على الجهات التي تستخدم OVHcloud CLI التحقق مما إذا كان أحد قد نزل الأداة أو حدّثها خلال فترة التعرض. وفي حال حدوث تنزيل، يُعامل الجهاز على أنه معرّض للخطر وتُدوّر الأسرار المخزنة عليه. وتبيّن الإجراءات أدناه ترتيبًا عمليًا للعمل.

ما يجب فعله الآن

1. تحديد أي تنزيل أو تحديث لأداة OVHcloud CLI من GitHub يوم 19 أكتوبر بين 12:47 و14:21 بتوقيت UTC، بالاستعانة بسجلات الوكيل والأجهزة الطرفية وخطوط CI.
2. اعتبار أي جهاز شغل نسخة من تلك الفترة مخترقًا محتملًا، وعزله وتدوير بيانات الاعتماد والرموز والمفاتيح المخزنة عليه.
3. مراجعة نشاط حسابات السحابة المرتبطة بتلك الأسرار بحثًا عن أي وصول غير متوقع.
4. إعادة تثبيت الأداة فقط من نسخة تؤكد إرشادات OVHcloud سلامتها.
5. توثيق الحادثة ضمن إجراءات مخاطر الأطراف الثالثة وسلسلة التوريد وإحاطة قيادة الأمن بها.