

إصدارات OVHcloud CLI من 0.11.0 إلى 0.15.0 ملغمة عبر حساب GitHub مخترق



أعلنت OVHcloud أن مهاجمين استخدموا حساب GitHub مخترقاً لنشر إصدارات ملغمة من أداة CLI (من 0.11.0 إلى 0.15.0) تسرق الأسرار من القرص. على من شغلها تنظيف الجهاز وإلغاء جميع الأسرار.

- عُدلت الإصدارات من 0.11.0 إلى 0.15.0 من OVHcloud CLI، بينما الإصداران 0.10.0 و0.16.0 سليمان.
- ظهر الإصدار الخبيث الساعة 14:47 يوم 19 أكتوبر وتم رصده وحجبه الساعة 16:21 بعد بلاغ من أحد العملاء.
- كان إعداد عدم قابلية تعديل الإصدارات (release immutability) في GitHub معطلاً، ما أتاح لحساب ذي صلاحيات كافية تعديل إصدارات قائمة دون المرور بفحوص CI/CD.
- تربط OpenSourceMalware الهجوم بحملة GlassWorm؛ والمنصات المتأثرة هي macOS وLinux وWindows، بينما لم تتأثر البنى من المصدر ولا صور Docker.

- كل من شغل ملفاً تنفيذياً متأثراً عليه اعتبار جميع الأسرار على ذلك الجهاز مختربة.

حذرت OVHcloud مستخدميها من أن أداة سطر الأوامر مفتوحة المصدر التي توفرها لإدارة خدمات السحابة والاستضافة وأتمتة المهام جرى العبث بها لتوزيع برمجية خبيثة تسرق المعلومات. وبحسب الرئيس التنفيذي للشركة Octave Klaba، سيطر مهاجم على حساب GitHub لأحد المطورين، ووصل إلى مستودع الأداة، وعدّل الإصدارات من 0.11.0 إلى 0.15.0.

ما الذي حدث

ظهر الإصدار المخترق الساعة 14:47 يوم 19 أكتوبر، ورُصد وحُجب الساعة 16:21 بعد بلاغ من أحد العملاء. أما الإصدار 0.10.0 والإصدار الأحدث 0.16.0 فهما سليمان. ووصف Klaba البرمجية الخبيثة بأنها رديئة الصنع، لكن هدفها كان استخراج الأسرار من القرص.

وأوضحت الشركة لاحقاً أن إعداد عدم قابلية تعديل الإصدارات في GitHub كان معطلاً، ما سمح لحساب ذي صلاحيات كافية بتغيير إصدارات قائمة دون المرور بفحوص CI/CD. وتؤكد الشركة أن خطوط CI/CD، بما فيها الاختبارات وكشف الثغرات، لم تتأثر. وقد فُغلت الإعدادات المذكور وتعدّ الحادثة منتهية.

السياق الأوسع

ترجّح OpenSourceMalware، وهي منصة مجتمعية لاستخبارات التهديدات، أن الهجوم جزء من عملية جديدة لمجموعة GlassWorm. وتقول إن خطوط CI/CD لم يُعبث بها وإن الحزم المصابة بُنيت محلياً، وإن حساب GitHub المستخدم كان مخترقاً منذ أكثر من ستة أشهر. ولم يحلل الباحثون الحمولة الخبيثة نفسها. والمنصات المتأثرة هي ARMg macOS (Intel وARM64 Linux وx86_64 وWindows x86-64، ولم تتأثر البنىات من المصدر ولا صور Docker.

المطلوب

ينبغي للجهات التي تستخدم الأداة التحقق من الإصدار المثبت وتاريخ تثبيته. وعلى من شغل ملفاً تنفيذياً متأثراً تنظيف النظام وإلغاء كل الأسرار المخزنة عليه، وفق توصية الشركة.

ما يجب فعله الآن

1. حصر محطات العمل وخوادم البناء وخوادم القفز التي تستخدم OVHcloud CLI وتحديد ما تُبِت عليه أحد الإصدارات من 0.11.0 إلى 0.15.0.
2. التحديث إلى الإصدار 0.16.0 أو إزالة الأداة من الأجهزة المتأثرة؛ فالإصدار 0.10.0 والبنىات من المصدر وصور Docker غير متأثرة.
3. في أي جهاز شغل عليه ملف تنفيذي متأثر، تنظيف النظام وإلغاء وتدوير جميع الأسرار على قرصه، ومنها مفاتيح API والرموز ومفاتيح SSH.
4. مراجعة نشاط حساب OVHcloud للبيانات المعنية ومراقبة أي استخدام غير متوقع.
5. تفعيل عدم قابلية تعديل الإصدارات في GitHub وفرض المصادقة متعددة العوامل ومبدأ الصلاحيات الأدنى على الحسابات والمستودعات التي تديرها فرقكم.

6. تسجيل الحادثة في سجل مخاطر الأطراف الثالثة وسلسلة التوريد، واتباع إجراءات الإبلاغ عن الحوادث إذا تعرضت أسرار للانكشاف.