اختراق قناة تحديثات cPGuard لزرع باب خلفي في خوادم Linux



اخترق مهاجم نظام تحديثات cPGuard في 2 نوفمبر ودفع سكربتاً خبيثاً إلى خوادم Linux لدى العملاء، فثبّت باباً خلفياً وجمع تجزئات كلمات المرور وملفات حساسة، وفق بيان الشركة المطورة OPSSHIELD.

- اخترق المهاجم نظام تحديثات cPGuard في 2 نوفمبر.
- وصل السكربت الخبيث إلى خوادم Linux لدى العملاء عبر قناة التحديث الرسمية.
- ثبّت السكربت باباً خلفياً على الخوادم التي نفذته وجمع تجزئات كلمات المرور وملفات حساسة.
- تفيد OPSSHIELD بأن المهاجم استولى فعلًا على جزء من البيانات المجمعة.
- ورد ذكر الإصدار cPGuard 5.88.25 وما بعده في المصدر بشكل مبتور، لذا يجب التحقق من النطاق الدقيق في بيان الشركة.

ما الذي حدث

وفق الشركة المطورة OPSSHIELD، تمكن مهاجم من الوصول إلى نظام التحديثات الخاص بأداة الحماية cPGuard في 2 نوفمبر، واستغل ذلك الوصول لتوزيع سكربت خبيث على خوادم Linux لدى العملاء.

وقد ثُبّت باب خلفي على الخوادم التي نفذت السكربت، كما جمع السكربت تجزئات كلمات المرور وملفات حساسة أخرى. وتذكر OPSSHIELD أن المهاجم استولى منذ ذلك الحين على جزء من هذه البيانات.

أهمية الحادثة

تمثل الحادثة اختراقاً لسلسلة التوريد، إذ وصل الكود الخبيث عبر قناة يثق بها مديرو الأنظمة وغالباً ما تُمنح صلاحيات مرتفعة. وأدوات الأمن هدف حساس بصورة خاصة لأنها تعمل على الخوادم التي يُفترض أن تحميها. كما يمكن كسر تجزئات كلمات المرور أو إعادة استخدامها لاحقاً، فقد يستمر الخطر حتى بعد إزالة الباب الخلفي.

النص المتاح من المصدر مبتور عند الإشارة إلى cPGuard 5.88.25 والإصدارات اللاحقة، ولذلك لا يمكننا تحديد الإصدارات أو التثبيتات المتأثرة. يُرجع في هذه التفاصيل إلى بيان OPSSHIELD.

النهج الموصى به

على الجهات التي تشغّل cPGuard التعامل مع الأمر كحادثة محتملة لا كتحديث اعتيادي: التحقق من التعرض أولًا، ثم التحقيق والاحتواء، مع افتراض أن بيانات الاعتماد على الخوادم المتأثرة قد تكون مكشوفة إلى أن يثبت العكس.

ما يجب فعله الآن

1. حصر جميع الخوادم التي تشغّل cPGuard ومراجعة بيان OPSSHIELD لتأكيد الإصدارات المتأثرة ومؤشرات الاختراق.
2. التحقق مما إذا جرى سحب تحديثات في 2 نوفمبر أو بعده، وفحص تلك الخوادم بحثاً عن السكربت وآليات بقاء غير معروفة واتصالات خارجية غير متوقعة.
3. عزل أي خادم تظهر عليه علامات اختراق مع حفظ السجلات والأدلة القرصية قبل إعادة البناء.
4. تدوير كلمات المرور والمفاتيح وبيانات اعتماد الخدمات للحسابات على الخوادم المتأثرة، على افتراض تسرب التجزئات.
5. التصعيد وفق إجراءات الاستجابة للحوادث وتقييم التزامات الإبلاغ للجهات التنظيمية مثل الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي، ونظام حماية البيانات الشخصية إن وُجدت بيانات شخصية.
6. إيقاف التحديث التلقائي لأدوات الأمن من أطراف ثالثة على الخوادم الحرجة إلى أن تؤكد الشركة سلامة القناة.