Hex لإدارة الحزم تُبلغ عن اختراق خوادمها وتطلب من المستخدمين إعادة ضبط بيانات الدخول



أعلنت Hex، مدير الحزم للغتي Elixir وErlang، أن مهاجمين نفّذوا أوامر على خوادمها عبر ثغرة حرجة. لم يُرصد تعديل على الحزم، لكن لا يمكن استبعاد الوصول إلى قاعدة البيانات، ويُنصح المستخدمون بإعادة ضبط كلمات المرور والمصادقة الثنائية.

- في 23 نوفمبر استغل مهاجمون ثغرة إلغاء تسلسل بيانات غير موثوقة دون مصادقة (CVE-2026-129514، بدرجة CVSS 10) في hex.pm لتنفيذ أوامر على نظام التشغيل.
- تفيد Hex بأن الهجوم أُوقف وأُصلح الخلل خلال 20 دقيقة، بعد 69 طلباً خبيثاً طالت ستة خوادم ويب.
- لا دليل على تعديل الحزم أو تغيير قاعدة البيانات أو بقاء المهاجم داخل الأنظمة، لكن لا يمكن استبعاد الاطلاع على البريد الإلكتروني وتجزئات كلمات المرور ومفاتيح API والجلسات وأسرار المصادقة الثنائية.

- غيّرت Hex بيانات اعتماد التخزين وCDN والبريد وقاعدة البيانات ومفاتيح التوقيع، ما أدى إلى تسجيل خروج جميع المستخدمين.
- عولج الصنف نفسه من الثغرات في Ash Framework db_connectiong وflopg.

ما الذي حدث

أفصحت Hex، مدير الحزم للغتي Elixir وErlangg، عن وصول غير مصرح به إلى خوادم الويب الخاصة بها في 23 نوفمبر. استغل المهاجمون ثغرة إلغاء تسلسل بيانات غير موثوقة دون مصادقة في hex.pm، وهي CVE-2026-129514 بدرجة CVSS تبلغ 10، عبر طلب مُعدّ بصيغة Erlang external term format أتاح تنفيذ أوامر عن بُعد.

بين 18:16 و18:29 بالتوقيت العالمي أرسل المهاجم 69 طلباً خبيثاً طالت ستة خوادم. استبدلت Hex جميع الخوادم بنسخ مُحدَّثة عند 18:30، وحجبت قاعدة جدار الحماية حركة المهاجم بالكامل عند 18:33.

المعروف وغير المعروف

لم تجد Hex دليلًا على تعديل غير مصرح به للحزم أو تغيير في قاعدة البيانات أو بقاء المهاجم داخل الأنظمة. غير أنها لا تستطيع استبعاد الوصول إلى محتويات القاعدة، ومنها عناوين البريد الإلكتروني وتجزئات كلمات المرور وتجزئات مفاتيح API والجلسات وأسرار المصادقة الثنائية وسجلات التدقيق. وأي قراءة من خادم مخترق ستبدو مشروعة، كما أن قراءات قاعدة البيانات والوثائق الخاصة لا تُسجَّل، ما يحد من الرؤية.

ولأن أوامر المهاجم كانت قادرة على قراءة بيانات اعتماد الخوادم، استبدلت Hex بيانات اعتماد التخزين وCDN والبريد وقاعدة البيانات ومفاتيح توقيع الجلسات والرموز، وسُجّل خروج جميع المستخدمين من hex.pm وعملاء Hex.

وتأثر Ash Framework بالصنف نفسه من الثغرات، وصدر إصلاحه في 24 نوفمبر تحت CVE-2026-124283، كما عولجت ثغرات مرتبطة في db_connection (CVE-2026-133555) وflop (CVE-2026-130411).

توجيهات Hex

على أصحاب الحسابات تغيير كلمات مرور hex.pm وإعادة ضبط المصادقة الثنائية. وإلى حين صدور إصدارات جديدة من العميل، ينبغي جلب الحزم من repo.hex.pm فقط وتجنب المرايا الخارجية. ويجب الحذر من الرسائل التي تدّعي أنها من Hex والتحقق من أن الروابط تؤدي إلى hex.pm.

ما يجب فعله الآن

1. حصر مشاريع Elixir/Erlang وخطوط CI/CD التي تستخدم Hex، وتحديد الحسابات ومفاتيح API العائدة للمنشأة.
2. إلزام جميع أصحاب حسابات hex.pm بتغيير كلمات المرور وإعادة ضبط المصادقة الثنائية، وتدوير مفاتيح API الخاصة بـ Hex احترازياً.
3. قصر جلب الحزم على repo.hex.pm وحجب المرايا الخارجية إلى حين صدور عملاء Hex المحدّثين.
4. تحديث Ash Framework db_connectiong وflopg إلى النسخ المُصلحة ومراجعة الشيفرة بحثاً عن إلغاء تسلسل غير آمن لمدخلات غير موثوقة.

5. تنبيه الموظفين إلى رسائل التصيد المنتحلة لـ Hex وطلب التحقق من الروابط مقابل hex.pm.
6. عند احتمال تأثر بيانات شخصية، تقييم الالتزامات بموجب نظام حماية البيانات الشخصية (PDPL) وإجراءات الاستجابة للحوادث الداخلية.