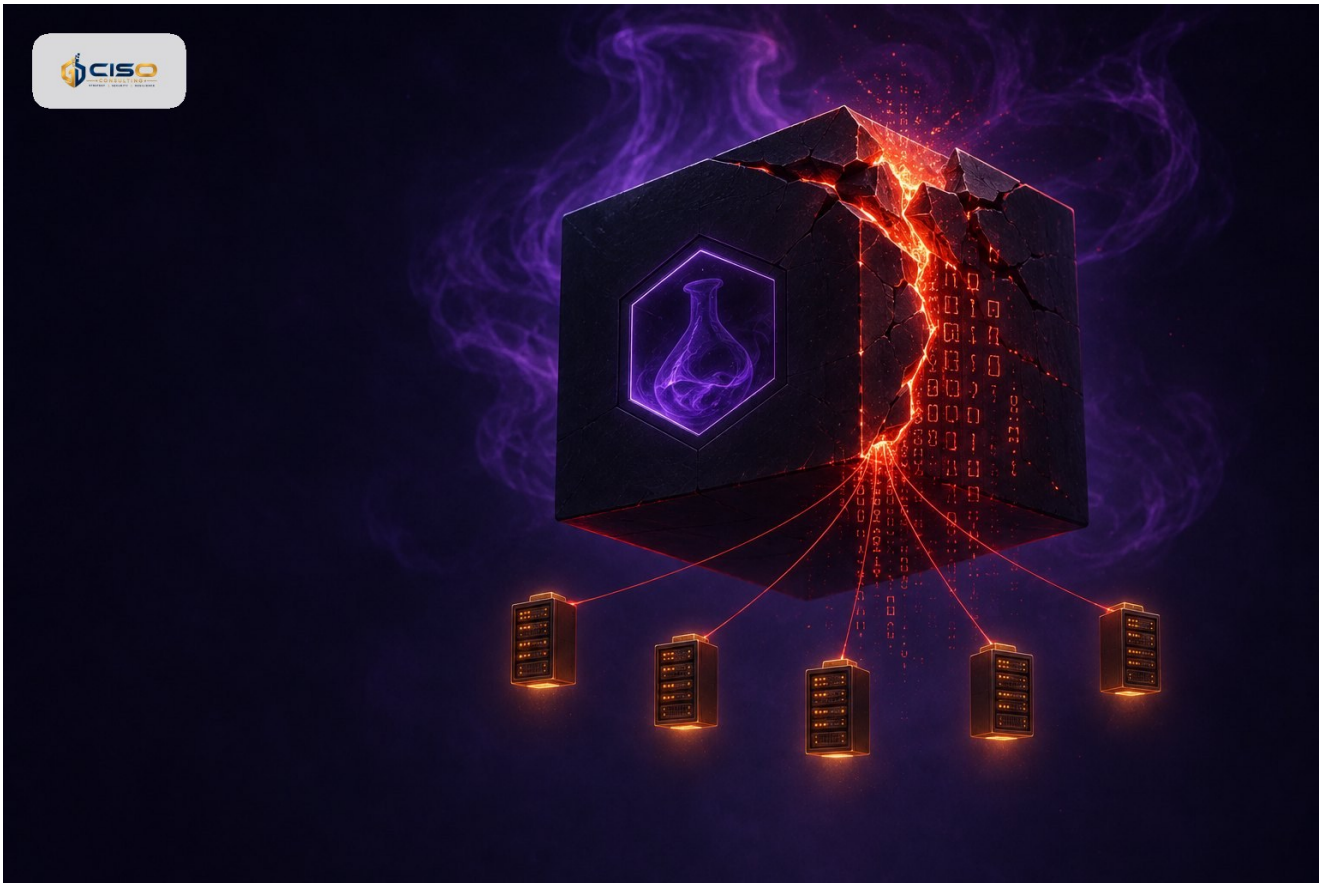
ثغرة تنفيذ أوامر عن بُعد بتقييم CVSS 10.0 في سجل حزم Hex.pm واختراق ستة خوادم



نفّذ مهاجم أوامر على نظام التشغيل في ستة خوادم إنتاج تابعة لـ Hex.pm، سجل الحزم الذي يعتمد عليه مطورو Elixir وErlang. يعود الخلل إلى فبراير 2016، وأصلحه القائمون عليه خلال نحو 15 دقيقة.

- اختُرقت ستة خوادم إنتاج لـ Hex.pm عبر ثغرة تنفيذ أوامر عن بُعد بتقييم CVSS 10.0.
- نفّذ المهاجم أوامر على نظام التشغيل في الخوادم يوم الاثنين.
- كان الكود الضعيف موجوداً في السجل منذ فبراير 2016.
- وضع القائمون على الخدمة جميع الخوادم على نسخة مُصلحة خلال نحو 15 دقيقة من أول طلب خبيث.

ما الذي حدث

نفّذ مهاجم أوامر على نظام التشغيل في ستة خوادم إنتاج تابعة لـ Hex.pm، وهو سجل الحزم الذي يجلب منه مطورو Elixir وErlang اعتماديات مشاريعهم. والثغرة من نوع تنفيذ الأوامر عن بُعد وتقييمها CVSS 10.0، وهو أعلى تقييم في المقياس.

كان الخلل موجوداً في كود السجل منذ فبراير 2016. وتحرّك الفريق القائم على الخدمة سريعاً، إذ أصبحت جميع الخوادم على نسخة مُصلحة خلال نحو 15 دقيقة من أول طلب خبيث.

أهمية الخبر

تقع سجلات الحزم في بداية سلسلة توريد البرمجيات. فالجهات التي تطوّر تطبيقات بلغتي Elixir وErlang تسحب الشيفرة من Hex.pm إلى بيئات التطوير والبناء لديها، ولذلك يعنيها اختراق السجل، مع أن المصدر يصف الهجوم بأنه استهدف خوادم السجل نفسها.

لا يذكر المصدر ما إذا كانت حزم منشورة قد عُدّلت، ولا يورد رقم CVE أو تفاصيل تقنية إضافية. لذا ينبغي عدم الجزم بما يتجاوز المؤكد.

النهج الموصى به

على الفرق التي تستخدم Elixir أو Erlang اعتبار الخبر دافعاً لمراجعة آلية الحصول على الاعتماديات والتحقق منها، ومتابعة بيانات القائمين على الخدمة الرسمية لأي إرشادات بشأن الحزم أو بيانات الاعتماد المتأثرة. فالمراجعة الهادئة المبنية على الأدلة لنشاط الاعتماديات الأخير أنفع من القلق الواسع.

ما يجب فعله الآن

1. حدّد المشاريع وخطوط البناء الداخلية التي تعتمد على حزم Hex.pm.
2. تابع إعلانات القائمين على Hex.pm الرسمية للاطلاع على أي إرشادات بشأن الحزم أو بيانات الاعتماد المتأثرة.
3. راجع تحديثات الاعتماديات الأخيرة في مشاريع Elixir وErlang بحثاً عن تغييرات غير متوقعة.
4. ثبّت إصدارات الاعتماديات وتحقق من قيم التجزئة أو ملفات القفل في خطوط البناء.
5. أدرج سجلات المصادر المفتوحة ضمن تقييم مخاطر الأطراف الثالثة وسلسلة التوريد.