# OpenAI وCisco تطلقان Shirudo، أداة مفتوحة المصدر لحماية أنظمة Linux غير المحدّثة



أطلقت OpenAI وCisco أداة Shirudo مفتوحة المصدر تعتمد على eBPF لتطبيق "دروع" مؤقتة تمنع استغلال الثغرات في Linux إلى حين تثبيت التصحيحات، دون إعادة تشغيل الخدمات.

- تستخدم Shirudo تقنية eBPF لنشر حمايات مؤقتة ومحددة تسمى "الدروع" دون إعادة تشغيل الأنظمة.
- يمكن لوكلاء الذكاء الاصطناعي المساعدة في فحص الثغرات وإعداد الدروع، مع بقاء قرار النشر بيد الإنسان.
- تُوقَّع الدروع تشفيرياً، وتسجّل وحدات TPM وقت تحميلها أو إزالتها.
- في الاختبارات، منع درع مخصص محاولة استغلال Java4Shell ضد خدمة Elasticsearch قيد التشغيل دون تعطيلها.
- حذّر باحث من Expel من ترك وكلاء الذكاء الاصطناعي يكتبون قواعد قد تؤثر في النواة.

أطلقت OpenAI وCisco أداة Shirudo، وهي أداة أمنية مفتوحة المصدر لأنظمة Linux تهدف إلى تقليص التعرض للخطر في الفترة بين اكتشاف الثغرة وتثبيت التصحيح. وتطبّق الأداة حمايات مؤقتة في وقت التشغيل تُسمى "دروعاً"، دون إعادة تشغيل الخدمات.

## آلية العمل

تعتمد Shirudo على eBPF، وهي آلية في Linux تشغّل برامج خاضعة للرقابة داخل النواة دون تعديل شيفرتها المصدرية أو إعادة التشغيل. وتستهدف الدروع السلوك الخبيث بدقة بحيث تستمر عمليات التطبيقات المشروعة. ويمكن للمشغّلين تقييم أثر الدرع قبل فرضه، كما تتوفر لهم أعداد الإصابات التي تبيّن محاولات الاستغلال.

يستطيع وكلاء الذكاء الاصطناعي فحص الثغرات وإعداد الدروع والتحقق منها، بينما يبقى قرار النشر بيد الإنسان. والدروع موقّعة تشفيرياً ويفحصها مدقق eBPF وضوابط النواة، وتوفر وحدات TPM سجلات يمكن التحقق منها لتحميل الدروع وإزالتها. ويذكر المطورون أن الأداة تُفعَّل من سطر الأوامر ولا تحتاج إلى خدمة تعمل باستمرار. وتخطط الجهتان لتوزيع دروع مختبرة في حزم موقّعة عبر سجل OCI.

## تحفظات

في الاختبارات، منع باحثو OpenAI وCisco محاولة استغلال Java4Shell ضد خدمة Elasticsearch قيد التشغيل دون تعطيلها. ويرى Marcus Hutchins من Expel إمكانات كبيرة في eBPF، لكنه يتحفظ على ترك وكلاء الذكاء الاصطناعي يكتبون قواعد قد تؤثر في النواة، ويشير إلى أن النهج يقتصر على Linux. والدرع حل مؤقت وليس بديلًا عن التصحيح.

وحددت OpenAI ندوة تقنية عبر الإنترنت في 15 ديسمبر.

## ما يجب فعله الآن

1. حدّدوا خوادم Linux التي يتأخر تصحيحها بسبب نوافذ التغيير أو متطلبات التشغيل المستمر، وسجّلوها كمرشحة لضوابط تعويضية.
2. قيّموا Shirudo في بيئة اختبار قبل أي استخدام إنتاجي، بما في ذلك أثرها على سلوك التطبيقات المشروعة.
3. اشترطوا موافقة بشرية وإدارة تغيير لأي درع يولَّد بالذكاء الاصطناعي بما يتوافق مع إجراءات التغيير والمخاطر لديكم.
4. تعاملوا مع الدروع كإجراءات تخفيف مؤقتة وتابعوا تثبيت التصحيحات حتى الإغلاق.
5. تحققوا من إمكانية الاستفادة من توقيع الدروع وسجلات TPM كأدلة للتدقيق والمراقبة.