ملخص التهديدات الأسبوعي: ثغرات PHP وGitLab وLinux وNode.js وحادثة LiteLLM ضمن أبرز العناوين



يرصد ملخص ThreatsDay أسبوعًا حافلاً: ثغرات RCE حرجة في PHP وGitLab، وأخطاء في Linux، وشهادات eMudhra مخترقة، وثغرة في Node.js، وإصدار LiteLLM مخترق، وعقد Tor مختطفة.

- أُبلغ عن ثغرات تنفيذ تعليمات عن بُعد حرجة في PHP وGitLab.
- تضمّن الأسبوع أخطاء أمنية خطيرة في Linux وثغرة RCE في Node.js.
- أُفيد باختراق شهادات eMudhra.
- تعرّض إصدار من LiteLLM للاختراق، واختُطفت مئات عقد Tor.
- تشمل العناوين أيضًا تسرّب أسرار متعلقة بالذكاء الاصطناعي، وسرقة شيفرة PingCAP، وثغرة في Signal، وتجاوزًا للمصادقة في Laravel.

يصف ملخص ThreatsDay الأسبوعي من The Hacker News أيامًا مزدحمة لفرق الأمن، إذ ظهرت عدة أخبار مهمة قبل انتهاء الأسبوع.

ما الذي رُصد

تشمل العناوين الرئيسة ثغرات تنفيذ تعليمات عن بُعد (RCE) حرجة في PHP وGitLab، وأخطاء أمنية خطيرة في Linux، وثغرة RCE في Node.js. وإلى جانب الثغرات، يشير الملخص إلى اختراق شهادات eMudhra، وإصدار مخترق من LiteLLM، واختطاف مئات عقد Tor.

ويذكر عنوان الخبر أيضًا تسرّب أسرار متعلقة بالذكاء الاصطناعي، وسرقة شيفرة مصدرية من PingCAP، وثغرة في Signal مرتبطة بإنهاء المكالمات، وتجاوزًا للمصادقة في Laravel، مع 21 خبرًا آخر. والمقتطف المتاح لنا لا يتضمن تفاصيل تقنية أو إصدارات متأثرة أو أرقام CVE أو حلولاً لأي منها، لذا ينبغي الرجوع إلى التقرير الأصلي وإشعارات الموردين قبل اتخاذ أي إجراء.

لماذا يهم ذلك

تتنوع العناصر بين أطر تطوير الويب ومنصات المطورين وأنظمة التشغيل وبنية الشهادات وأدوات الذكاء الاصطناعي. وهذه مكونات شائعة في بيئات الجهات المنظمة، كما أن محوري سلسلة التوريد وتسرّب الأسرار يعنيان كل جهة تستخدم حزمًا مفتوحة المصدر أو مكتبات ذكاء اصطناعي.

المنهج المقترح

يُفضَّل التعامل مع الملخص كدافع لمراجعة الجرد لا كحالة طارئة. تأكدوا من المنتجات المذكورة التي تستخدمونها، واطلعوا على إشعارات الموردين، وأعطوا الأولوية للأنظمة المكشوفة على الإنترنت ومسارات التطوير.

ما يجب فعله الآن

1. راجعوا سجل الأصول بحثًا عن PHP وGitLab وNode.js وLinux وLaravel وLiteLLM وحددوا الإصدارات المستخدمة.
2. اطلعوا على إشعارات الموردين وطبّقوا التحديثات المتاحة، بدءًا بالأنظمة المكشوفة على الإنترنت.
3. تحققوا من مصدر وسلامة LiteLLM وغيرها من حزم الذكاء الاصطناعي والمصدر المفتوح المستخدمة في البناء.
4. تحققوا من استخدام شهادات صادرة عن eMudhra واتبعوا توجيهات الجهة المصدرة.
5. افحصوا المستودعات ومسارات CI بحثًا عن أسرار مكشوفة وبدّلوا ما يُعثر عليه.