

eMudhra تلغي ثماني شهادات وسيطة ضعيفة المفاتيح والمتصفحات تحجبها



ألغت eMudhra ثماني شهادات وسيطة لأن مفاتيحها الخاصة يمكن استرجاعها بسهولة. حجبتها المتصفحات الرئيسية، لكن البرامج ذات مخازن الثقة الخاصة قد تبقى تثق بها حتى تُحدَّث.

- استخدمت الشهادات الثماني مفاتيح P-384 أنشئت في أبريل 2025 بقيم أقل من 256، فيمكن استرجاعها بتجربة 256 رقماً فقط.
- عزت eMudhra الخلل إلى خطأ في سكرت التوليد اختيرت بسببه مفاتيح أضعف للتوقيع، ولم تجد دليلاً على إصدار شهادات للمستخدمين النهائيين.
- حجبت Mozilla و Chrome الشهادات في 17 أكتوبر و Apple في 19 أكتوبر، وصدر Firefox 158.0.1 في 20 أكتوبر.
- قد تبقى البرامج ذات مخازن الشهادات الخاصة أو التي لا تفحص الإلغاء تثق بها، وعالجت Go المشكلة ضمن CVE-2026-111943.

ما الذي حدث

ألغت جهة إصدار الشهادات eMudhra ثماني شهادات وسيطة بعد أن اكتشف باحث في 17 أكتوبر أن مفاتيحها الخاصة شديدة الضعف. ووفق تقرير Mozilla عن الحادثة، أنشئت مفاتيح P-384 في أبريل 2025 بقيم أقل من 256، فيمكن لأي شخص استرجاعها بتجربة 256 احتمالاً فقط. وأظهر مثال منشور أن قيمة أحد المفاتيح لا تتجاوز 4. وتحققت BleepingComputer من أن المفتاح المنشور يطابق إحدى الشهادات الملغاة.

أرجعت eMudhra المشكلة إلى خطأ في سكربت التوليد أنتج مجموعة ثانية من المفاتيح الأضعف، واختيرت للتوقيع خطأً لتشابه تسمياتها مع المفاتيح السليمة. كما أرسلت بعض الشهادات إلى Sectigo للتوقيع المتقاطع. وتقول الشركة إن معظم الشهادات الوسيطة لم تُستخدم في الإنتاج ولم تجد دليلاً على إصدار شهادات لمستخدمين نهائيين. كان إساءة الاستخدام ممكنة منذ أبريل 2025، دون دليل على حدوثها.

استجابة الجهات المطورة

حجبت Mozilla الشهادات عبر OneCRL في 17 أكتوبر دون الحاجة إلى تحديث المتصفح. وحجبت Chrome في اليوم نفسه الشهادات الوسيطة الست المخولة بإصدار شهادات TLS، وأضافت Apple حمايتها في 19 أكتوبر. وأصدرت Mozilla الإصدار 158.0.1 Firefox وتحديثات ESR في 20 أكتوبر للإصدارات التي لم تتلقَّ الإلغاء المبكر.

يبقى التعرض في البرامج التي تحتفظ بمخازن شهادات خاصة أو لا تفحص الإلغاء. وأصدرت Go الإصدارين 1.27.3 و 1.26.10 معالجة لـ CVE-2026-111943. ويعرض موقع تتبع أعدّه مهندس Mozilla دينيس جاكسون البرامج المتأثرة والتحديثات، ويحذر من أن أداة `usr/bin/curl/` المدمجة في macOS قد تظل تثق بالشهادات.

الأهمية

قد تتيح الشهادات المزورة انتحال مواقع مشروعة واعتراض الاتصالات المشفرة. المتصفحات مغطاة في الغالب، أما الثغرات المحتملة فتقع في التطبيقات والخوادم والحاويات.

ما يجب فعله الآن

1. حصر التطبيقات والخوادم والحاويات وصور البناء التي تضم مخازن شهادات خاصة أو لا تفحص الإلغاء.
2. تطبيق تحديثات حزم الشهادات وبيئات التشغيل المدرجة في موقع التتبع، ومنها Go 1.27.3 أو 1.26.10 عند الاقتضاء.
3. تحديث Firefox إلى 158.0.1 أو إصدار ESR الحالي، والتأكد من حداثة Chrome وأجهزة Apple.
4. استخدام نقاط الاختبار في النشرة لمعرفة الأنظمة التي ما زالت تثق بالشهادات الوسيطة الملغاة.
5. عدم الاعتماد على أداة `usr/bin/curl/` المدمجة في macOS للمهام الحساسة للثقة إلى حين معالجتها.
6. توثيق العملية في سجلات إدارة الشهادات والثغرات.