

اختراق مفاتيح ثمانية شهادات وسيطة لدى eMudhra واستجابة عاجلة من مزوّدي المتصفحات



أكدّت Mozilla وبرنامج Chrome Root Program من Google في 20 أكتوبر اختراق المفاتيح الخاصة لثمانية شهادات وسيطة لدى eMudhra، ما يتيح إصدار شهادات لأي موقع تقبلها المتصفحات.

- أكدّت Mozilla وبرنامج Chrome Root Program من Google الاختراق في 20 أكتوبر.
- يشمل الأمر ثمانية شهادات وسيطة لدى eMudhra.
- تُوقع الجهة الوسيطة الشهادات التي تعرضها المواقع، لذا يمكن لحائز المفتاح إصدار شهادة لأي موقع تقبله المتصفحات.
- أبلغ باحث عن المشكلة، وتشير المصدر إلى إصلاحات طارئة في المتصفحات والبرمجيات.

ما الذي حدث

أكدت Mozilla وبرنامج Chrome Root Program من Google في 20 أكتوبر أن المفاتيح الخاصة لثماني شهادات وسيطة تابعة لجهة إصدار الشهادات eMudhra قد جرى اختراقها. وقد أبلغ باحث عن المشكلة، وتشير المصدر إلى صدور إصلاحات طارئة في المتصفحات والبرمجيات.

لماذا يهم ذلك

توقع الجهة الوسيطة (Intermediate CA) الشهادات التي تعرضها المواقع على المستخدمين. وعليه، يستطيع من يملك أحد المفاتيح المخترقة إصدار شهادة لأي موقع، وستقبلها المتصفحات. ويضعف ذلك الثقة التي تقوم عليها اتصالات TLS، وقد يتيح انتحال المواقع أو اعتراض الحركة.

لا يتضمن المقتطف المتاح تفاصيل إضافية عن الشهادات المحددة أو نطاق إساءة الاستخدام أو مواعيد الإصلاح، ولذلك ينبغي الرجوع إلى تحديثات المزودين لمعرفة المزيد.

الخطوات العملية

يتمثل الإجراء العملي في تطبيق تحديثات المتصفحات والبرمجيات فور صدورهما، والتحقق مما إذا كانت بيئتك تثق بشهادات مرتبطة بسلسلة eMudhra. وعلى الفرق المسؤولة عن مخازن الثقة والوكلاء (Proxies) وتثبيت الشهادات (Certificate Pinning) مراجعتها الآن دون انتظار وقوع حادث.

ما يجب فعله الآن

1. تطبيق تحديثات المتصفحات وأنظمة التشغيل وبرمجيات الأمن فور صدورهما من المزودين.
2. التحقق من وجود أنظمة داخلية أو موجهة للعملاء تثق بشهادات مرتبطة بسلسلة eMudhra أو تستخدمها.
3. مراجعة مخازن الثقة ووكلاء فحص TLS وإعدادات تثبيت الشهادات.
4. متابعة إشعارات المزودين وبرامج الجذور للاطلاع على النطاق وتفاصيل المعالجة.
5. إدراج حوادث الثقة بالشهادات في خطط الاستجابة للحوادث إن لم تكن مشمولة.