اختراق ثلاثة سجلات نطاقات وطنية للحصول على شهادات HTTPS لنطاقات تابعة لجوجل



أعلنت جوجل أن مهاجمين اخترقوا سجلات النطاقات .gh و.sl و.as وحصلوا على شهادات HTTPS غير مصرّح بها لعدة نطاقات تابعة لها. لم تُخترق أنظمة جوجل، لكن النطاقات المنتهية بهذه اللواحق الثلاث تعرّضت للخطر.

- أعلنت جوجل في 6 أكتوبر أن مهاجمين اخترقوا ثلاثة نطاقات وطنية عليا: .gh (غانا) و.sl (سيراليون) و.as (ساموا الأمريكية).
- حصل المهاجمون على شهادات HTTPS غير مصرّح بها لعدة نطاقات تابعة لجوجل.
- لم تتعرض أنظمة جوجل نفسها للاختراق.
- تعرّض أي نطاق ينتهي بـ .gh أو .sl أو .as للخطر.
- قد تتيح الشهادة المزوّرة للمهاجم انتحال الموقع الأصلي عبر اتصال مشفّر.

ما الذي حدث

أعلنت جوجل في 6 أكتوبر أن مهاجمين اخترقوا ثلاثة نطاقات وطنية عليا هي: .gh الخاص بغانا، و.sl الخاص بسيراليون، و.as الخاص بساموا الأمريكية. ومن خلال هذا الوصول حصلوا على شهادات HTTPS غير مصرّح بها لعدة نطاقات تابعة لجوجل.

وأكدت جوجل أن أنظمتها لم تُخترق، وأن الخلل كان على مستوى السجلات، ما عرّض أي نطاق ينتهي بـ .gh أو .sl أو .as للخطر.

لماذا يهم الأمر

تتيح الشهادة الصالحة لنطاق ما لحاملها انتحال الموقع الحقيقي عبر اتصال مشفّر، ولن يرى المستخدم تحذيرًا واضحًا لأن الشهادة تبدو سليمة. وتبيّن الحادثة أن الثقة في HTTPS تعتمد جزئيًا على أمن سجلات النطاقات وإجراءات التحقق من ملكية النطاق، وهي أطراف خارج محيط المنظمة.

لا يوضح المصدر كيف جرى اختراق السجلات، ولا عدد الشهادات الصادرة، ولا ما إذا تأثرت جهات أخرى. لذلك ينبغي التعامل مع التفاصيل بحذر إلى حين صدور معلومات إضافية.

ما ينبغي النظر فيه

من غير المرجح أن تتعرض المؤسسات في المملكة مباشرة ما لم تمتلك نطاقات بهذه اللواحق أو تعتمد عليها. ومع ذلك تمثّل الحادثة فرصة لمراجعة سجل النطاقات ومراقبة الشهادات والاعتماديات على الأطراف الخارجية، والتأكد من جاهزية الفريق للتصرف عند اكتشاف شهادة مزوّرة لأحد نطاقاته.

ما يجب فعله الآن

1. تحقق مما إذا كانت مؤسستك أو موردوها الرئيسيون يمتلكون نطاقات تنتهي بـ .gh أو .sl أو .as أو يعتمدون عليها.
2. راجع سجلات شفافية الشهادات (Certificate Transparency) لنطاقاتك، وتأكد من وجود تنبيه عند إصدار أي شهادة غير متوقعة.
3. احتفظ بسجل شامل للنطاقات وجهات التسجيل وحسابات السجلات، مع تفعيل المصادقة متعددة العوامل على حسابات التسجيل.
4. فكّر في استخدام سجلات CAA لتحديد جهات إصدار الشهادات المسموح لها بإصدار شهادات لنطاقاتك.
5. أدرج اكتشاف الشهادات المزوّرة في خطة الاستجابة للحوادث، بما يشمل خطوات الإلغاء والإشعار.