

ثغرة تجاوز سعة المخزن المؤقت في مفاتيح Zyxel GS1900 Series



تتيح ثغرة تجاوز سعة المخزن المؤقت في مفاتيح Zyxel GS1900 Series للمهاجمين غير المصادق عليهم على الشبكة المحلية تنفيذ أوامر نظام التشغيل عبر طلبات HTTP مصممة خصيصاً.

- تؤثر الثغرة CVE-2026-7273 على مفاتيح Zyxel GS1900 Series عبر تجاوز سعة المخزن المؤقت في برنامج CGI
- يمكن للمهاجمين غير المصادق عليهم على الشبكة المحلية استغلال الثغرة عبر طلبات HTTP مصممة خصيصاً
- قد يتيح الاستغلال الناجح تنفيذ أوامر نظام التشغيل بشكل تعسفي
- يجب على المؤسسات تطبيق تحديثات الجهة المصنعة أو التوقف عن استخدام المنتج في حال عدم توفر حلول
- ينبغي لمالكي الأصول تقييم التعرض للإنترنت وتحديد أولويات التصحيح بناءً على المخاطر

نظرة عامة على الثغرة

تحتوي مفاتيح الشبكة من سلسلة Zyxel GS1900 على ثغرة تجاوز سعة المخزن المؤقت القائم على المكسب المتعقبة برقم CVE-2026-7273. تكمن الثغرة في مكون برنامج CGI للأجهزة المتأثرة ويمكن استغلالها من قبل مهاجم غير مصادق عليه يمتلك وصولاً إلى الشبكة المحلية. من خلال إرسال طلب HTTP مصمم خصيصاً إلى مفتاح معرض للخطر، قد يتمكن المهاجم من تفعيل حالة تجاوز المخزن المؤقت وربما تنفيذ أوامر نظام تشغيل تعسفية على الجهاز.

لا تتطلب الثغرة مصادقة، مما يخفض حاجز الاستغلال أمام الجهات التهديدية التي حصلت على موطئ قدم في الشبكة الداخلية. وهذا يجعل الثغرة مثيرة للقلق بشكل خاص للمؤسسات التي تنشر مفاتيح الشبكة في بيئات ذات تجزئة شبكية محدودة أو حيث تشكل التهديدات الداخلية اعتباراً مهماً.

المخاطر على المؤسسات السعودية

تواجه المؤسسات الخاضعة للتنظيم في المملكة التي تستخدم مفاتيح Zyxel GS1900 Series في بنيتها التحتية الشبكية مخاطر تشغيلية وامتثالية. قد يؤدي الاستغلال الناجح إلى اختراق سلامة الشبكة أو تمكين الحركة الجانبية داخل البيئة أو تسهيل استخراج البيانات. يجب على المؤسسات الخاضعة للضوابط الأساسية للأمن السيبراني للهيئة الوطنية للأمن السيبراني أو إطار الأمن السيبراني لمؤسسة النقد العربي السعودي معاملة هذه الثغرة كأولوية تصحيح.

يجب على مالكي الأصول تقييم ما إذا كانت المفاتيح المتأثرة معرضة لقطاعات شبكية غير موثوقة أو للإنترنت، وتقييم التأثير المحتمل على الأنظمة الحرجة وتدفقات البيانات.

الاستجابة الموصى بها

ينبغي للمؤسسات تحديد جميع مفاتيح Zyxel GS1900 Series في بيئتها فوراً وتطبيق التصحيحات أو الحلول المقدمة من الجهة المصنعة دون تأخير. إذا لم تكن التصحيحات متاحة أو لا يمكن تطبيقها بسرعة، يُنصح بعزل الأجهزة المتأثرة أو التوقف عن استخدامها حتى يصبح الإصلاح ممكناً. يجب مراجعة تجزئة الشبكة وضوابط الوصول للحد من تعرض واجهات الإدارة للمسؤولين الموثوقين فقط.

ما يجب فعله الآن

1. تحديد جميع مفاتيح Zyxel GS1900 Series المنشورة في البنية التحتية الشبكية لديكم
2. تطبيق التصحيحات الأمنية أو الحلول المقدمة من الجهة المصنعة فور توفرها
3. تقييم تعرض المفاتيح المتأثرة للإنترنت والشبكات غير الموثوقة وعزلها عند الضرورة
4. مراجعة تجزئة الشبكة لضمان أن واجهات الإدارة متاحة فقط للمسؤولين المصرح لهم
5. التوقف عن استخدام الأجهزة المتأثرة إذا لم تكن التصحيحات متاحة ولا يمكن تخفيف المخاطر
6. توثيق إجراءات المعالجة والجدول الزمنية لإعداد تقارير الامتثال للهيئة الوطنية للأمن السيبراني أو مؤسسة النقد العربي السعودي حسب الاقتضاء