مفاتيح Zyxel GS1900: التحديث السابق لا يوقف الثغرة المستغلة وإصدار جديد متاح



أفادت Binarly بأن مفاتيح Zyxel GS1900 التي طُبّق عليها التحديث السابق ما زالت عرضة لاستغلال نشط للثغرة. وأصدرت Zyxel برمجية جديدة لـ10 طرازات.

- وجد باحثو Binarly أن إصلاح Zyxel السابق لا يمنع الاستغلال الذي استخدمه المهاجمون.
- تتيح الثغرة لأي جهة تصل إلى واجهة الإدارة عبر الويب تنفيذ أوامر دون تسجيل الدخول.
- الثغرة مستغلة فعلياً في هجمات.
- أصدرت Zyxel برمجية جديدة لـ10 طرازات من GS1900 تسد الثغرة.
- يشير المصدر إلى أن الإصلاح السابق هو الإصدار 2.90.

ما الذي اكتُشف

أفاد باحثون في Binarly بأن مفاتيح الشبكة Zyxel GS1900 التي طُبّق عليها إصلاح الشركة السابق لثغرة مستغلة فعلياً ما زالت قابلة للاستهداف بالاستغلال نفسه. ويحدد المصدر الإصلاح السابق بأنه الإصدار 2.90. وعملياً قد يبقى مفتاح تم تحديثه ومعالجته في السجلات عرضة للخطر.

تتيح الثغرة لأي جهة تستطيع الوصول إلى واجهة الإدارة عبر الويب تنفيذ أوامر على الجهاز دون مصادقة. ولأن الثغرة مستغلة بالفعل، فإن إتاحة هذه الواجهة هي مصدر القلق الرئيسي.

ما فعلته Zyxel

أصدرت Zyxel برمجية جديدة لـ10 طرازات من GS1900 تسد الثغرة. ولا يذكر مقتطف المصدر الطرازات المتأثرة ولا أرقام الإصدارات الجديدة ولا معرّف CVE، لذا ينبغي للفرق استقاء هذه التفاصيل من إشعار الشركة المصنّعة.

لماذا يهم ذلك

تقع مفاتيح الشبكة في صميم الاتصال الداخلي، وقد يمنح اختراق أحدها المهاجم موطئ قدم داخل الشبكة. وعلى الجهات التي أغلقت هذا البند بعد التحديث السابق إعادة فتحه والتحقق من إصدار البرمجية المثبّت فعلياً.

ما يجب فعله الآن

1. حصر جميع مفاتيح Zyxel GS1900 والتأكد من الطراز وإصدار البرمجية المثبّت.
2. اعتبار الأجهزة المحدّثة بالإصلاح السابق فقط ما زالت معرّضة للخطر، وإعادة فتح طلب المعالجة.
3. تطبيق البرمجية الجديدة من Zyxel على الطرازات المتأثرة بعد الاختبار ووفق إجراءات إدارة التغيير.
4. حصر الوصول إلى واجهة الإدارة عبر الويب في شبكة إدارة مخصصة ومنعه من شبكات المستخدمين والإنترنت.
5. مراجعة سجلات المفاتيح وإعداداتها بحثاً عن أوامر أو تغييرات غير متوقعة، وتصعيد أي نتائج وفق إجراءات الاستجابة للحوادث.