Zyxel تصلح ثغرة يوم الصفر المستغلة في نحو 1000 محوّل من سلسلة GS1900



أصدرت Zyxel تصحيحاً لثغرة يوم الصفر في محوّلات GS1900 التي استُغلت لاختراق نحو 1000 جهاز حول العالم وسرقة ملفات الإعداد وبيانات الاعتماد. يُنصح بتطبيق التحديث ومراجعة التعرض.

- أصدرت Zyxel تصحيحاً لثغرة يوم صفر في محوّلات الشبكة من سلسلة GS1900.
- استُغلت الثغرة فعلياً قبل توفر التصحيح.
- أُفيد باختراق نحو 1000 جهاز حول العالم.
- سرق المهاجمون ملفات الإعداد وبيانات الاعتماد من المحوّلات المتأثرة.
- المقتطف المتاح من المصدر لا يذكر رقم CVE ولا تفاصيل تقنية كاملة.

أصدرت Zyxel تصحيحاً لثغرة يوم صفر تؤثر في محوّلات الشبكة من سلسلة GS1900. ووفق ما نشره موقع

BleepingComputer، استغل مهاجمون الثغرة لاختراق نحو 1000 جهاز حول العالم.

ما الذي أُفيد به

استخدم المهاجمون الثغرة لسرقة ملفات الإعداد وبيانات الاعتماد من المحوّلات. ولأن الاستغلال سبق توفر التصحيح، ربما تعرضت بعض الجهات قبل أن تتاح لها فرصة الاستجابة.

المقتطف المتاح لنا من التقرير لا يتضمن رقم CVE ولا إصدارات البرنامج الثابت المتأثرة ولا الآلية التقنية للهجوم. لذلك ينبغي للفرق الرجوع إلى نشرة Zyxel والتقرير الأصلي لمعرفة هذه التفاصيل وعدم افتراضها.

أهمية الأمر

قد تكشف ملفات إعداد المحوّلات وبيانات الاعتماد بنية الشبكة والحسابات الإدارية والأنظمة المتصلة. وإذا سُرقت، فإن تحديث الجهاز يغلق منفذ الدخول لكنه لا يعالج وحده أثر انكشاف تلك البيانات السرية.

المقاربة المقترحة

ابدؤوا بتحديد ما إذا كانت محوّلات GS1900 موجودة في بيئتكم، بما في ذلك الفروع والمواقع التي تديرها أطراف ثالثة. طبّقوا التصحيح، ثم اعتبروا بيانات الاعتماد المخزنة على هذه الأجهزة أو المستخدمة معها معرّضة للانكشاف إلى أن يثبت خلاف ذلك. فالمراجعة الهادئة والمنظمة أفضل من استبدال عاجل غير مخطط.

ما يجب فعله الآن

1. حصر جميع محوّلات Zyxel من سلسلة GS1900، بما فيها الموجودة في الفروع والتي تديرها أطراف ثالثة.
2. الاطلاع على نشرة Zyxel وتطبيق التصحيح الصادر على الأجهزة المتأثرة.
3. تغيير كلمات مرور الحسابات الإدارية وغيرها من بيانات الاعتماد المخزنة على هذه المحوّلات أو المستخدمة معها.
4. حصر واجهات الإدارة في شبكات إدارية مخصصة وتجنب تعريضها للإنترنت.
5. مراجعة سجلات المحوّلات والشبكة بحثاً عن تنزيلات إعداد أو عمليات دخول غير متوقعة، وتصعيد النتائج عبر إجراءات الاستجابة للحوادث.