تقارير عن استغلال ثغرة في سحابة GL.iNet لاختراق أجهزة الراوتر وأجهزة KVM



أفاد موقع BleepingComputer أن مهاجمين يستغلون ثغرة في خدمة GL.iNet السحابية لإصابة أجهزة الراوتر وأجهزة KVM. تعذّرت قراءة نص المقال، لذا لم تتأكد التفاصيل الفنية.

- المشكلة المبلّغ عنها ثغرة في خدمة GL.iNet السحابية.
- يُقال إن مهاجمين يستغلونها لإصابة أجهزة الراوتر وأجهزة KVM.
- نص المصدر غير مقروء، فلا يمكن تأكيد رقم CVE أو الطرازات المتأثرة أو حالة التصحيح.
- على الجهات التي تستخدم أجهزة GL.iNet مراجعة إشعارات المورّد الرسمية.

ما الذي ورد في التقرير

نشر موقع BleepingComputer تقريراً بعنوان «Hackers exploit GL.iNet cloud flaw to infect routers, KVM

devices». ويُفهم من العنوان أن مهاجمين يستغلون ضعفاً في خدمة GL.iNet السحابية لاختراق نوعين من الأجهزة: أجهزة الراوتر وأجهزة KVM التي تتيح التحكم عن بُعد بلوحة المفاتيح والشاشة والفأرة في أجهزة أخرى.

ما لا يمكننا تأكيده

لم يكن نص المقال مقروءاً عند إعداد هذا الخبر. لذلك لا يمكننا تحديد طبيعة الثغرة، ولا ما إذا كان قد أُسند لها رقم CVE، ولا الطرازات أو إصدارات البرنامج الثابت المتأثرة، ولا ما يفعله المهاجمون بعد الإصابة، ولا توفر إصلاح من عدمه. تركنا هذه النقاط دون تخمين، ويُعد هذا الخبر إشعاراً أولياً وليس تقييماً كاملًا.

أهمية الموضوع

تقع أجهزة الراوتر وأجهزة KVM في نقاط حساسة من الشبكة. فاختراق الراوتر قد يكشف حركة البيانات، واختراق جهاز KVM قد يمنح المهاجم تحكماً عن بُعد في الأنظمة خلفه. وتُستخدم هذه الأجهزة أحياناً في الفروع الصغيرة والمواقع البعيدة والمختبرات خارج إشراف تقنية المعلومات المركزي، فيسهل إغفالها.

الخطوات المقترحة

ابدأوا بمعرفة ما إذا كانت أجهزة GL.iNet مستخدمة لديكم، بما في ذلك الفروع والعاملون عن بُعد. ثم اتبعوا إرشادات المورّد والتقرير الأصلي للحصول على التفاصيل المؤكدة، وطبّقوا أي تحديث منشور بعد التحقق منه.

ما يجب فعله الآن

1. حصر جميع أجهزة الراوتر وKVM من GL.iNet، بما في ذلك الفروع والمواقع البعيدة وبيئات العمل من المنزل.
2. مراجعة إشعارات GL.iNet الرسمية وتقرير BleepingComputer الأصلي لمعرفة الطرازات المتأثرة والإصلاحات.
3. تطبيق تحديثات المورّد فور تأكيدها، مع الاختبار عند ارتباط الجهاز بعمليات حرجة.
4. حصر الإدارة عن بُعد والإدارة السحابية لهذه الأجهزة بالحد اللازم ومراجعة حسابات الإدارة.
5. فحص السجلات وإعدادات الأجهزة بحثاً عن تغييرات غير متوقعة، وعزل أي جهاز يُشتبه في اختراقه.