اختراق سحابة GoodCloud من GL.iNet وزرع برمجيات خبيثة في الراوترات وأجهزة KVM



اخترق مهاجمون خدمة GoodCloud للإدارة عن بُعد من GL.iNet وزرعوا برمجيات خبيثة في راوترات وأجهزة KVM المتصلة بها. أُصلح خلل السحابة، لكن الأجهزة المصابة تبقى كذلك حتى تحديث البرنامج الثابت وفحصها.

- اكتشفت GL.iNet في 20 نوفمبر 2026 أن GoodCloud تعرضت للاختراق عبر ثغرة سحابية لم تفصّل طبيعتها، وقد أُصلحت.
- إصلاح جانب السحابة لا ينظّف الأجهزة المصابة؛ أما أحدث برنامج ثابت مستقر فيزيل هذه البرمجية تحديداً دون إعادة ضبط المصنع.
- نطاق الحادث ما زال قيد التحديد، بما في ذلك تأثر الحواسيب المتصلة بأجهزة KVM المصابة.
- أفادت شريكتها RemoteToHome Consulting بأن 166 من 199 راوتراً وصلت إليه أظهرت هجوم 20 نوفمبر أو بوابة خلفية أقدم أو كليهما.

- امتلك المهاجم صلاحيات root في بعض الحالات، فقد تكون المفاتيح وكلمات المرور والملفات الشخصية على الجهاز قد نُسخت.

اخترق مهاجمون خدمة GoodCloud، وهي خدمة الإدارة عن بُعد السحابية التابعة لـ GL.iNet، واستخدموها لتثبيت برمجيات خبيثة على راوترات وأجهزة KVM المرتبطة بها. ولا تزال الشركة تحقق في الحادث ولم تذكر عدد الأجهزة المتأثرة.

ما أعلنته GL.iNet

رصدت الشركة الاختراق في 20 نوفمبر 2026، وتقول إن الثغرة السحابية التي لم تصفها قد أُصلحت. غير أن هذا الإصلاح لا ينظّف الأجهزة التي أُصيبت بالفعل. وتنصح الشركة بتثبيت أحدث برنامج ثابت أمني مستقر، فهو يزيل هذه البرمجية تحديداً ولا يستلزم إعادة ضبط المصنع.

ومؤشر الاختراق المنشور لديها هو عملية تعمل بالصيغة crond -i /tmp/.log. وأضافت لاحقاً أن هناك مؤشرات أخرى لا تكشفها فحوصاتها السريعة الرسمية، وأشارت إلى سكربت من المجتمع للكشف الإضافي والتنظيف، محذرة من أن أياً من الطريقتين لا يضمن خلو الجهاز من الاختراق. وفي حال إصابة جهاز KVM، ينبغي فحص الحاسوب المتصل به بحثاً عن برامج أو إضافات متصفح أو حسابات غير مألوفة، وعناصر بدء تشغيل ومهام مجدولة وأنشطة شبكة غير معتادة.

ما وجده الشريك

فحصت RemoteToHome Consulting، وهي شريك خدمات لدى GL.iNet، الراوترات التي تديرها. ومن بين 199 راوتراً وصلت إليها، أظهر 166 هجوم 20 نوفمبر أو بوابة خلفية أقدم أو كليهما. ولم تتمكن من تحديد كيفية وصول البوابات الأقدم. كما نشرت تحليلًا لثغرة حقن أوامر في عميل GoodCloud ترجح استغلالها، ولم تؤكد GL.iNet ذلك بعد.

ولأن المهاجم امتلك صلاحيات root، تحذر الشركة من احتمال نسخ المفاتيح وكلمات المرور والملفات الشخصية المخزنة، وأن إعادة تثبيت الراوتر لا تعالج ذلك، إذ يجب سحب الصلاحيات من الطرف الآخر.

ما يجب فعله الآن

1. حصر راوترات وأجهزة KVM من GL.iNet المستخدمة، بما فيها المسجلة في GoodCloud، في المكاتب والفروع وأجهزة العاملين عن بُعد.
2. تثبيت أحدث برنامج ثابت مستقر على الأجهزة المتأثرة وتشغيل فحوصات GL.iNet وقائمة مؤشرات RTH معاً.
3. اعتبار أي جهاز مؤكد الإصابة مكشوفاً: تدوير المفاتيح وكلمات المرور وبيانات اعتماد VPN المخزنة عليه وسحب الصلاحيات من الأنظمة الأخرى.
4. فحص الحواسيب المتصلة بأجهزة KVM المصابة بحثاً عن برامج وحسابات ومهام مجدولة ونشاط شبكي غير مألوف.
5. تعطيل الإدارة السحابية عن بُعد في هذه الأجهزة حيثما لا تلزم، والالتزام بمتطلبات الإبلاغ عن الحوادث لدى الهيئة الوطنية للأمن السيبراني أو البنك المركزي السعودي عند تأكد الاختراق.