

ثغرة في سير العمل بنظام MikroTik RouterOS تتيح الوصول غير المصرح به للجلسات



يحتوي نظام MikroTik RouterOS على خلل في فرض سير العمل يتيح للعملاء غير المصرح لهم فتح جلسات وتنفيذ طلبات، ويمكن ربطه بثغرة أخرى للاستغلال.

- الثغرة CVE-2026-67279 تؤثر على نظام MikroTik RouterOS بسبب ضعف في فرض سير العمل السلوكي
- يمكن للمهاجمين غير المصرح لهم فتح قنوات الجلسات وإرسال طلبات التنفيذ
- يمكن ربط الثغرة مع CVE-2026-86060 لتحقيق استغلال غير مصرح به
- يجب تطبيق تدابير الحماية من المورد أو إيقاف استخدام المنتج في حال عدم توفر التحديثات
- على المؤسسات تقييم تعرض الأصول المتأثرة للإنترنت وإعطاء الأولوية للتحديثات الأمنية

نظرة عامة على الثغرة

تم اكتشاف ثغرة في نظام MikroTik RouterOS تتعلق **بالفرض غير السليم لسير العمل السلوكي** ومسجلة تحت الرقم CVE-2026-67279. يسمح هذا الخلل للعملاء غير المصرح لهم بفتح قنوات الجلسات وإرسال طلبات التنفيذ إلى الأجهزة المتأثرة. وهذا يمثل فشلاً كبيراً في التحكم بالوصول يتجاوز آليات المصادقة العادية.

تصبح الثغرة مثيرة للقلق بشكل خاص عند دمجها مع الثغرة CVE-2026-86060، حيث يمكن ربط الاثنتين معاً لتحقيق استغلال غير مصرح به لأنظمة RouterOS. يزيد نمط الهجوم هذا من مستوى المخاطر للمؤسسات التي تعتمد على بنية التوجيه من MikroTik.

متطلبات المعالجة

يجب على المؤسسات التي تشغل أجهزة MikroTik RouterOS تطبيق تدابير الحماية المقدمة من المورد فوراً. وفي حال عدم توفر التحديثات أو تدابير الحماية، ينبغي على المؤسسات إيقاف استخدام المنتج المتأثر حتى تصبح التحديثات الأمنية متاحة. تؤكد هذه الثغرة على أهمية الحفاظ على مستويات التحديث الحالية للبنية التحتية الشبكية.

تقع على عاتق أصحاب المصلحة مسؤولية إجراء تقييمات شاملة لمدى تعرض كل أصل للإنترنت. تواجه الأجهزة التي يمكن الوصول إليها مباشرة من الشبكات غير الموثوقة مخاطر مرتفعة ويجب إعطاؤها الأولوية في المعالجة. ينبغي على المؤسسات اتباع إرشادات التحديث القائمة على المخاطر والتأكد من نشر التحديثات الأمنية بشكل منهجي عبر بنيتها التحتية للتوجيه.

الاعتبارات التنظيمية

بالنسبة للمؤسسات الخاضعة للتنظيم في المملكة، تؤثر هذه الثغرة على البنية التحتية الشبكية الأساسية التي تدعم العمليات الحرجة. يجب الاحتفاظ بتوثيق مناسب لأنشطة التقييم والجداول الزمنية للمعالجة والضوابط التعويضية لإثبات الامتثال لأطر الأمن السيبراني المعمول بها.

ما يجب فعله الآن

1. إجراء جرد لجميع أجهزة MikroTik RouterOS عبر البنية التحتية الشبكية وتحديد حالة إصداراتها
2. تطبيق التحديثات الأمنية وتدابير الحماية المقدمة من المورد فوراً على جميع أنظمة RouterOS المتأثرة
3. تقييم مدى تعرض كل جهاز MikroTik للإنترنت وإعطاء الأولوية لمعالجة الأصول المواجهة للإنترنت
4. تنفيذ تجزئة الشبكة أو ضوابط الوصول للحد من تعرض أجهزة RouterOS حتى اكتمال التحديث
5. إيقاف استخدام الأجهزة المتأثرة في حال عدم توفر تدابير الحماية من المورد أو تعذر تطبيقها بسرعة
6. توثيق جميع أنشطة التقييم والمعالجة والضوابط التعويضية لأغراض الامتثال التنظيمي