

تنبيه حول ثغرة MikroTik RouterOS



تتيح ثغرة حرجية في إصدارات MikroTik RouterOS السابقة لـ 7.24 تنفيذ التعليمات البرمجية عن بُعد أو التسبب في انقطاع الخدمة. يجب على المؤسسات إعطاء الأولوية للتحديثات للتخفيف من المخاطر.

- تتيح الثغرة تنفيذ التعليمات البرمجية عن بُعد أو التسبب في انقطاع الخدمة.
- الإصدارات المتأثرة هي MikroTik RouterOS أقل من 7.24.
- تعود المشكلة إلى تجاوز عدد صحيح في معالجة طلبات HTTP.
- يمكن أن يحدث الاستغلال دون مصادقة.
- توصي MikroTik بالتحديث إلى الإصدار 7.24 أو أحدث.

نظرة عامة

تم تحديد ثغرة حرجية في إصدارات MikroTik RouterOS السابقة لـ 7.24. قد تمكن هذه الثغرة المهاجمين من تنفيذ

التعليمات البرمجية عن بُعد أو التسبب في انقطاع الخدمة. تنشأ المشكلة من تجاوز عدد صحيح في معالجة جسم طلب HTTP، والذي يمكن الوصول إليه قبل مصادقة المستخدم.

التأثير

يمكن أن يكون لاستغلال هذه الثغرة آثار خطيرة على المؤسسات التي تعتمد على إصدارات MikroTik RouterOS المتأثرة. يمكن لمهاجم غير مصدق استغلال هذه الثغرة للحصول على وصول جذر أو تعطيل الخدمات، مما يشكل مخاطر كبيرة على سلامة العمليات.

الإجراءات الموصى بها

لتخفيف المخاطر المرتبطة بهذه الثغرة، يُنصح المؤسسات باتخاذ الخطوات التالية:

- تحديث MikroTik RouterOS إلى الإصدار 7.24 أو أحدث.
- مراجعة ومراقبة تكوينات الشبكة بانتظام لرصد محاولات الوصول غير المصرح بها.
- تنفيذ تقسيم الشبكة لتقليل تعرض الأنظمة الحرجة.
- إجراء تقييمات للثغرات لتحديد وإصلاح نقاط الضعف المحتملة.
- البقاء على اطلاع على الإشعارات الأمنية من MikroTik والسلطات السيبرانية ذات الصلة.

ما يجب فعله الآن

1. تحديث MikroTik RouterOS إلى الإصدار 7.24 أو أحدث.
2. مراجعة ومراقبة تكوينات الشبكة بانتظام لرصد محاولات الوصول غير المصرح بها.
3. تنفيذ تقسيم الشبكة لتقليل تعرض الأنظمة الحرجة.
4. إجراء تقييمات للثغرات لتحديد وإصلاح نقاط الضعف المحتملة.
5. البقاء على اطلاع على الإشعارات الأمنية من MikroTik والسلطات السيبرانية ذات الصلة.