

ثغرة الكتابة خارج الحدود في نواة لينكس تتطلب تطبيق التحديثات الأمنية فوراً



ثغرة حرجية في مكون ebttables بنواة لينكس تسمح بالتلاعب غير المصرح به بالذاكرة، مما يستوجب تطبيق التحديثات الأمنية فوراً أو الانتقال من الأنظمة المنتهية الدعم.

- ثغرة كتابة خارج الحدود في مكون SNAT target ebttables بنواة لينكس
- تسمح الثغرة بإعادة كتابة عنوان الأجهزة لبروتوكول ARP والوصول إلى أجزاء ذاكرة المقبس غير الخطية
- المنتجات المتأثرة قد تكون منتهية الدعم أو الخدمة مع دعم محدود من المورد
- يجب على المؤسسات تطبيق تحديثات المورد أو التوقف عن استخدام الإصدارات غير المدعومة
- توصي CISA بالأولوية للتحديثات الأمنية بناءً على تعرض الأصول للإنترنت ومستوى المخاطر

نظرة عامة على الثغرة

تحتوي نواة لينكس على ثغرة كتابة خارج الحدود درجة تحمل الرقم التعريفي CVE-2026-53266 تؤثر على مكون ebttables SNAT target. يسمح العيب لعملية إعادة كتابة عنوان أجهزة مرسل بروتوكول ARP بالكتابة مباشرة في جزء ذاكرة مقبس غير خطي مدعوم بصفحة ملف مستوردة عبر splice، مما قد يتيح التلاعب غير المصرح به بالذاكرة. تشكل هذه الثغرة خطراً كبيراً على الأنظمة التي تشغل إصدارات نواة لينكس المتأثرة، خاصة تلك العاملة في بيئات الإنتاج التي تتعامل مع تصفية حركة الشبكة وترجمة العناوين.

قد تكون العديد من الأنظمة المتأثرة تعمل بإصدارات نواة منتهية الدعم أو الخدمة مع دعم محدود أو معدوم من المورد. يجب على المؤسسات التي تعتمد على توزيعات لينكس القديمة تقييم مدى تعرضها فوراً.

المخاطر على المؤسسات الخاضعة للتنظيم

بالنسبة للمؤسسات المالية ومقدمي الرعاية الصحية ومشغلي البنية التحتية الحيوية في المملكة، تمثل هذه الثغرة مخاطر تشغيلية وامتثالية. قد تكون الأنظمة التي تؤدي وظائف ترجمة عناوين الشبكة أو الجدار الناري أو تصفية الحزم باستخدام ebttables عرضة للخطر. يمكن أن يؤدي احتمال تلف الذاكرة إلى عدم استقرار النظام أو الوصول غير المصرح به أو انقطاع الخدمة مما يؤثر على الخدمات المقدمة للعملاء والعمليات الداخلية.

يجب على الجهات الخاضعة للتنظيم تقييم بنيتها التحتية لنظام لينكس مقابل نشرات المورد وتحديد الجداول الزمنية للتحديثات بناءً على أهمية الأصول ومدى تعرضها للإنترنت.

إرشادات المعالجة

يجب تطبيق تحديثات المورد فوراً حيثما كانت متاحة. بالنسبة للأنظمة منتهية الدعم، يجب على المؤسسات التخطيط للانتقال إلى إصدارات نواة مدعومة أو طول بديلة. تؤكد إرشادات CISA على تحديد الأولويات بناءً على المخاطر، مع اهتمام خاص بالأصول المعرضة للإنترنت والأنظمة التي تعالج بيانات حساسة. يجب على المؤسسات توثيق إجراءات المعالجة والحفاظ على الامتثال للأطر الأمنية المعمول بها التي تحكم تقوية الأنظمة وإدارة الثغرات.

ما يجب فعله الآن

1. جرد جميع أنظمة لينكس وتحديد إصدارات النواة التي تشغل ebttables أو وظائف ترجمة عناوين الشبكة
2. مراجعة النشرات الأمنية للموردين وتطبيق التحديثات المتاحة لثغرة CVE-2026-53266 فوراً على أنظمة الإنتاج
3. إعطاء الأولوية للتحديثات على الأصول المعرضة للإنترنت والأنظمة التي تعالج بيانات خاضعة للتنظيم وفقاً لتقييم المخاطر
4. وضع خطط انتقال لتوزيعات لينكس منتهية الدعم أو الخدمة إلى إصدارات مدعومة
5. توثيق جميع أنشطة المعالجة والاستثناءات لإعداد تقارير الامتثال للهيئة الوطنية للأمن السيبراني أو مؤسسة النقد العربي السعودي أو الجهات التنظيمية الأخرى
6. إجراء اختبارات التحقق بعد التحديث لضمان استقرار النظام واستمرار الامتثال للمتطلبات التشغيلية