مايكروسوفت تنشر إشعارًا عن ثغرة رفع الصلاحيات في نواة لينكس CVE-2026-62840



نشر مركز MSRC التابع لمايكروسوفت إدخالاً للثغرة CVE-2026-62840، وهي ثغرة رفع صلاحيات في نواة لينكس. لا يقدّم المصدر تفاصيل إضافية، لذا ينبغي مراجعة الإدخال مباشرة.

- نشر MSRC معلومات عن الثغرة CVE-2026-62840.
- صُنّفت الثغرة على أنها رفع صلاحيات في نواة لينكس.
- لا يذكر المصدر درجة الخطورة أو الإصدارات المتأثرة أو تفاصيل التصحيح.
- ينبغي متابعة إدخال MSRC لاستكشاف أي تحديثات تُضاف لاحقًا.

ما الذي نُشر

نشر مركز الاستجابة الأمنية في مايكروسوفت (MSRC) إدخالاً للثغرة CVE-2026-62840، موصوفة بأنها ثغرة رفع

صلاحيات في نواة لينكس. وحالة الإدخال: «تم نشر المعلومات».

ما الذي لا يزال غير معروف

لا يتضمن المصدر المتاح لنا سوى العنوان وحالة النشر. فلا يذكر درجة الخطورة، ولا إصدارات النواة أو التوزيعات المتأثرة، ولا ما إذا رُصد استغلال للثغرة، ولا ما إذا كان التصحيح متاحًا. لذلك لا نستخلص أي استنتاجات في هذه النقاط.

بوجه عام، تتيح ثغرة رفع الصلاحيات في نواة نظام التشغيل لمستخدم أو عملية محدودة الصلاحيات الحصول على صلاحيات أعلى على النظام المتأثر. ويعتمد الأثر الفعلي على تفاصيل لم يوفرها المصدر بعد.

الخطوات التالية

على الجهات التي تشغّل لينكس على الخوادم أو الأجهزة الافتراضية أو الحاويات أو الأجهزة المتخصصة أن تحدد مواقع هذه الأنظمة وأصحابها، ثم تتابع إدخال MSRC وإرشادات موردي توزيعات لينكس. ويُفضَّل ترتيب الأولويات بعد تأكيد الخطورة والإصدارات المتأثرة، وبما يتوافق مع إجراءات إدارة الثغرات والتغيير المعتمدة لديكم.

- تأكيد أصول لينكس الداخلة في النطاق.
- متابعة إدخال MSRC وقنوات الموردين.
- الاستعداد لاختبار التصحيحات ونشرها عند توفرها.

ما يجب فعله الآن

1. حصر خوادم لينكس والأجهزة الافتراضية والحاويات والأجهزة المتخصصة وتحديد مالك لكل منها.
2. متابعة إدخال MSRC للثغرة CVE-2026-62840 وإشعارات موردي توزيعات لينكس.
3. إدراج الثغرة في سجل الثغرات وتحديد أولويتها بعد تأكيد الخطورة والإصدارات المتأثرة.
4. تجهيز نافذة اختبار ونشر لتحديثات النواة ضمن إدارة التغيير.
5. مراجعة الوصول ذي الصلاحيات العالية والمراقبة على مضيفي لينكس الحرجة ريثما تتضح التفاصيل.