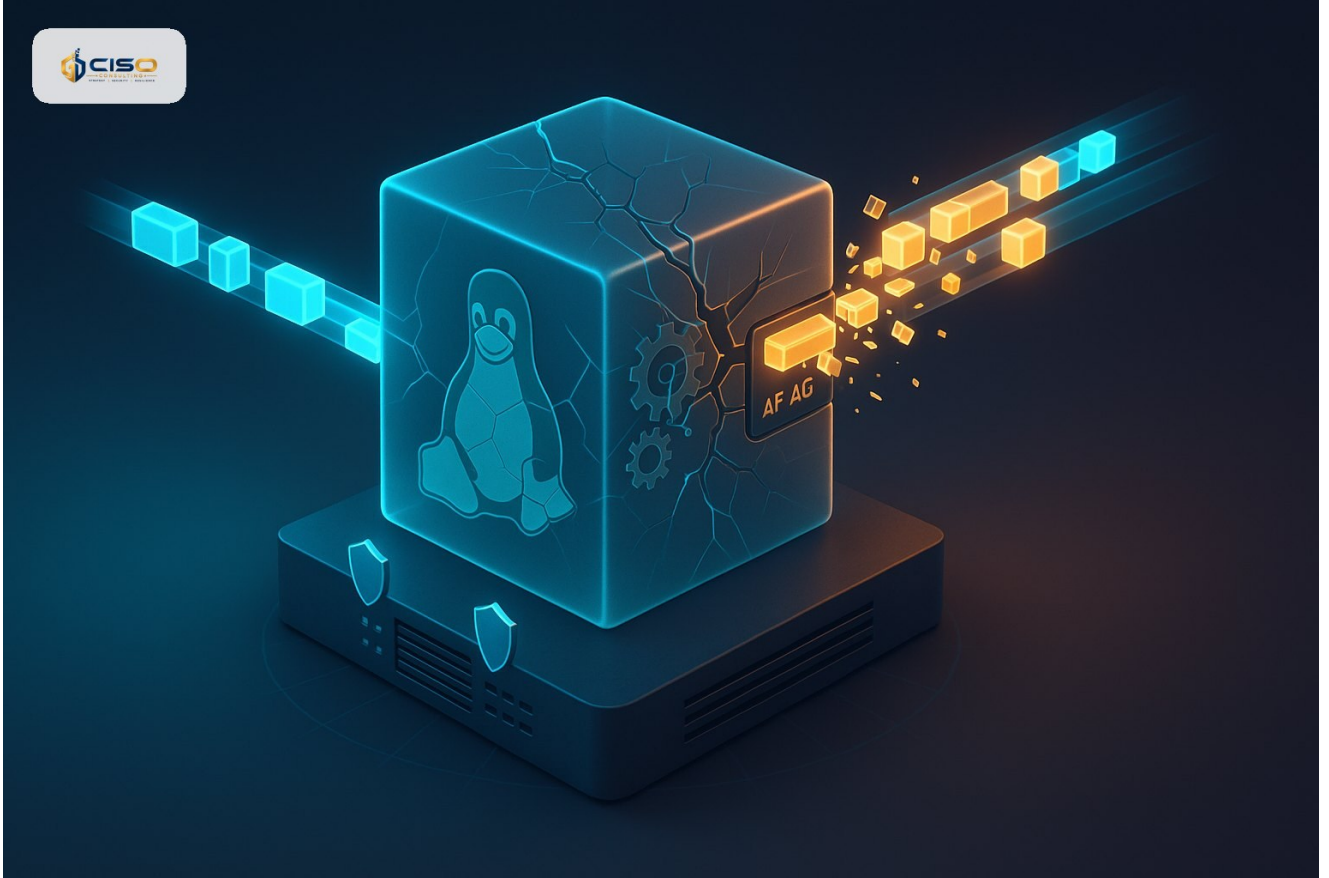


CVE-2025-39964: ثغرة تزامن في نواة Linux تخص مقابس AF_ALG



أدرجت CISA الثغرة CVE-2025-39964، وهي حالة تزامن في نواة Linux تتيح لعمليات كتابة متزامنة على مقبس AF_ALG واحد تداخل البيانات وإرباك حالته الداخلية. يُنصح بتطبيق معالجات المورّد وتقييم التعرض للإنترنت.

- الثغرة CVE-2025-39964 هي حالة تزامن (race condition) في نواة Linux.
- الكتابة المتزامنة على مقبس AF_ALG نفسه قد تؤدي إلى تداخل البيانات بصورة غير متوقعة.
- النتيجة اختلال في الحالة الداخلية للمقبس.
- تطلب CISA تطبيق معالجات المورّد وفق BOD 26-04 ومتطلبات الفرز الجنائي.
- الموعد المحدد للجهات الفيدرالية الأمريكية هو 21-09-2026، وعلى الجهات تقييم تعرض كل أصل للإنترنت.

ما الذي تم الإعلان عنه

أدرجت CISA الثغرة CVE-2025-39964، وهي حالة تزامن (race condition) في نواة Linux. فعند تنفيذ عدة عمليات كتابة في وقت واحد على مقبس AF_ALG واحد، قد تتداخل البيانات بصورة غير متوقعة، مما يترك الحالة الداخلية للمقبس غير متسقة.

لا يتناول المصدر سيناريو استغلال محددًا ولا إصدارات النواة المتأثرة ولا أثرًا يتجاوز هذا الاختلال، لذا ينبغي الرجوع إلى موّرد التوزيعة أو النظام للحصول على تفاصيل الإصدارات.

ما الذي تطلبه CISA

تطلب CISA تطبيق المعالجات وفق تعليمات الموّرد، بما يتوافق مع إرشادها BOD 26-04 بشأن ترتيب أولويات التحديثات الأمنية حسب المخاطر، ومع متطلبات الفرز الجنائي (Forensics Triage Requirements). وفي حال الخدمات السحابية تُتبع إرشادات BOD 26-04 المعمول بها. وإذا لم تتوفر معالجات فيوقف استخدام المنتج. والموعد المحدد للجهات الفيدرالية الأمريكية هو 21-09-2026.

وتقع على الجهات مسؤولية تقييم تعرض كل أصل للإنترنت والالتزام بإرشادات التحديث الواردة في BOD 26-04.

المنظور العملي للمؤسسات في المملكة

يخص الموعد النهائي الجهات الفيدرالية الأمريكية، لكنه مرجع مفيد لترتيب الأولويات. ولأن Linux منتشر في الخوادم والأجهزة والأحمال السحابية، فإن الخطوة الأولى معرفة أماكن تشغيله وأي الأصول متاح من الإنترنت. تُعالج هذه الأصول أولاً، وتُوثق القرارات، وتُحفظ الأدلة لأغراض التدقيق.

ما يجب فعله الآن

1. حصر خوادم Linux والأجهزة والأحمال السحابية وتحديد ما هو معرّض للإنترنت منها.
2. مراجعة نشرات موّرد Linux الخاصة بالثغرة CVE-2025-39964 وتطبيق المعالجات أو تحديثات النواة المتاحة.
3. إعطاء الأولوية للأصول المواجهة للإنترنت، مع اعتماد 21 سبتمبر 2026 مرجعًا للتخطيط.
4. عند غياب معالجة لمنتج ما، التخطيط لاستبداله أو إيقاف استخدامه.
5. توثيق قرارات التحديث والاستثناءات كأدلة لمراجعات ضوابط NCA ECC وإطار SAMA CSF.