Red Hat تصدر إصلاح ثغرة TCP في لينكس بدرجة 9.8 وإصلاحات Ubuntu لا تزال قيد الاختبار



صدرت نسخ نواة مصححة للثغرة CVE-2026-98432 في شيفرة IPv4 TCP بنواة لينكس لأنظمة RHEL 8 و9 و10، بينما لا تزال إصلاحات Ubuntu في قناة اختبار اختيارية.

- الثغرة CVE-2026-98432 من نوع use-after-free في شيفرة IPv4 TCP بنواة لينكس، وتبلغ درجتها 9.8.
- يمكن لمهاجم عن بُعد وبلا مصادقة الوصول إلى الثغرة.
- تتوفر نسخ نواة مصححة لأنظمة Red Hat Enterprise Linux 8 و9 و10.
- إصلاحات Ubuntu لأحدث ثلاثة إصدارات LTS متاحة فقط في قناة اختبار اختيارية.
- لم يُحدَّد موعد لتحديث Ubuntu المعتاد.

صدرت نسخ نواة مصححة لثغرة خطيرة في شيفرة IPv4 TCP ضمن نواة لينكس. الثغرة المعرّفة بالرقم CVE-2026-98432 هي من نوع use-after-free، وتبلغ درجة خطورتها 9.8.

ما هو معروف

يمكن لمهاجم عن بُعد ودون مصادقة الوصول إلى الثغرة، وهذا سبب ارتفاع تقييمها. وقد أصدرت Red Hat نسخ نواة مصححة لأنظمة Red Hat Enterprise Linux 8 و9 و10.

أما وضع Ubuntu فمختلف؛ فإصلاحات أحدث ثلاثة إصدارات LTS متاحة فقط في قناة اختبار اختيارية، ولم يُعلن موعد لتوفيرها عبر قناة التحديث المعتادة.

أهمية الأمر

تقع الشيفرة المعرّضة في حزمة الشبكة داخل النواة، لذا ينبغي مراجعة أي خادم لينكس يستقبل حركة IPv4 TCP. ونظرًا إلى أن نص المصدر مقتطع، لا تتناول هذه النشرة تفاصيل مثل حالة الاستغلال أو الأثر الدقيق، ويُنصح بالرجوع إلى نشرات المورّدين مباشرة.

المقاربة المقترحة

يمكن لبيئات Red Hat المضي في التحديث عبر إدارة التغيير المعتادة، مع إعطاء الأولوية للأنظمة المكشوفة لشبكات غير موثوقة. أما في Ubuntu فعلى الفرق أن تقرر بين استخدام إصلاحات قناة الاختبار على الأنظمة المكشوفة أو تطبيق ضوابط مؤقتة إلى حين صدور تحديث معتاد. وتتطلب تحديثات النواة عادةً إعادة تشغيل، لذا يجب التخطيط لنوافذ الصيانة مسبقًا.

ما يجب فعله الآن

1. حصر خوادم لينكس العاملة بـ RHEL 8 و9 و10 وإصدارات Ubuntu LTS، وتحديد ما هو مكشوف للإنترنت أو لشبكات غير موثوقة.
2. جدولة تحديثات نواة Red Hat ضمن إجراء التغيير الطارئ بدءًا بالأنظمة المكشوفة، والتخطيط لإعادة التشغيل اللازمة.
3. في Ubuntu، اتخاذ قرار قائم على قبول المخاطر بين استخدام إصلاحات قناة الاختبار على الأنظمة المكشوفة أو تطبيق قيود شبكية مؤقتة.
4. متابعة نشرات Ubuntu لحين صدور التحديث المعتاد وتطبيقه فور توفره.
5. توثيق حالة التعرض والمعالجة ضمن تقارير إدارة الثغرات.