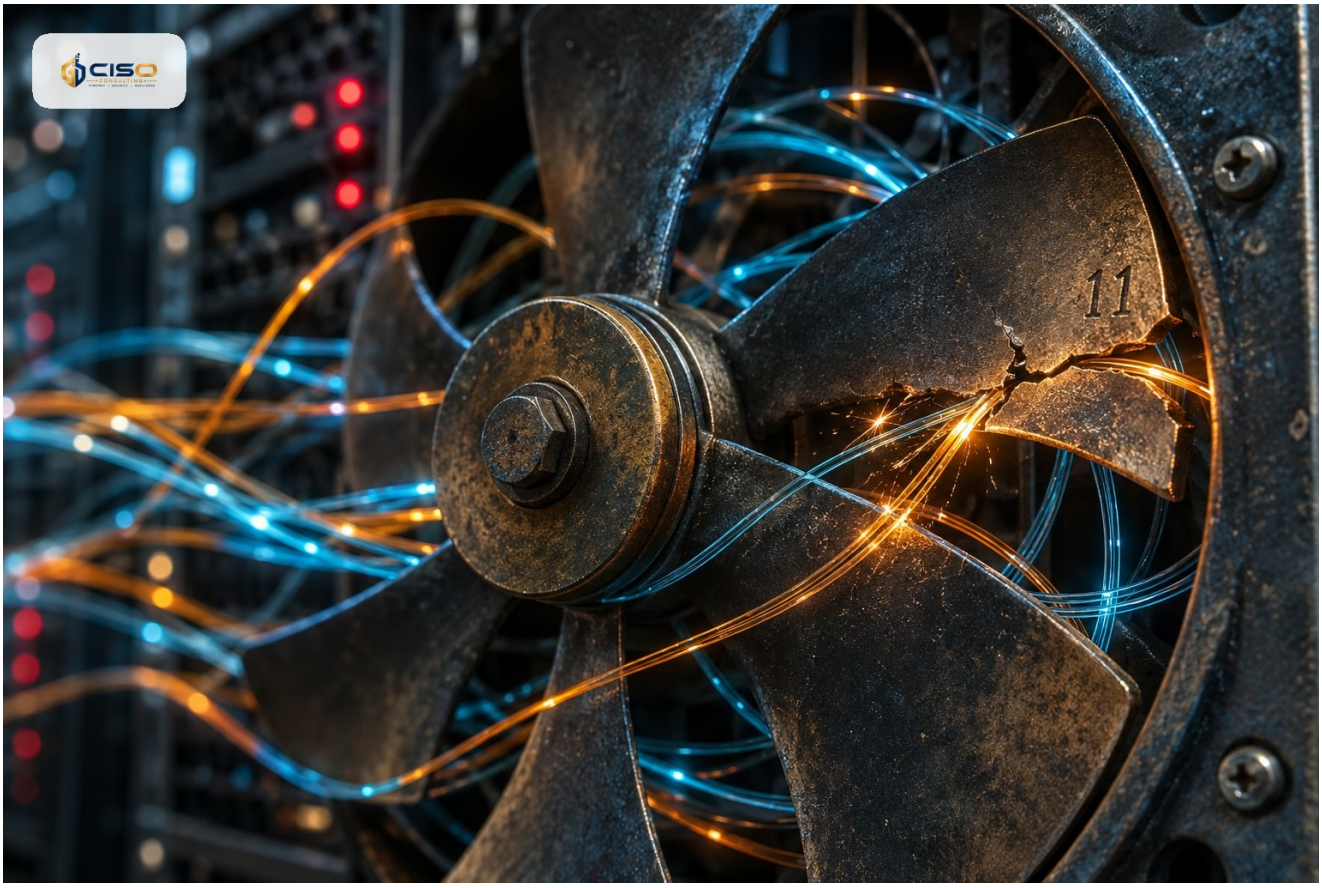
ثغرة NoisyTCP في نواة لينكس (CVE-2026-99288) تتيح إسقاط الخوادم عن بُعد



ثغرة عمرها 11 عامًا في نواة لينكس تُعرف بـ NoisyTCP (CVE-2026-99288) تتيح لمهاجم غير مصادَق إسقاط الخوادم بحزم TCP مصممة. التصحيح متاح، والحلول المؤقتة لها كلفة.

- الثغرة CVE-2026-99288 هي إشارة مؤشر فارغ (NULL pointer dereference) في نظام TCP بنواة لينكس وتمس معظم التوزيعات تقريبًا.
- يمكن استغلالها عن بُعد دون مصادقة، وينتج عنها انهيار النواة (kernel panic) وتوقف الخادم.
- وفق المصدر، لا تتيح تعديل البيانات ولا تنفيذ شيفرة عشوائية.
- نافذة التسابق ضيقة، لذا قد يستغرق استغلالها على خادم فعلي هادئ وقتًا طويلاً.
- دُمج الإصلاح في النواة الرئيسية قبل أسبوعين من النشر، ومن الحلول المؤقتة تعطيل SYN cookies أو حصر الاستقبال في طابور RX واحد.

ما الذي أُعلن

كشف الباحث Hyunwoo Kim عن ثغرة في نواة لينكس باسم **NoisyTCP** ورقمها CVE-2026-99288، عمرها 11 عامًا وتمس معظم توزيعات لينكس تقريبًا. ويمكن إسقاط الأنظمة التي تستقبل حزم TCP مباشرة وتشغّل Nginx أو Apache أو خادم SSH بإعداداتها الافتراضية.

الخلل هو إشارة إلى مؤشر فارغ (NULL pointer dereference) في نظام TCP بالنواة، ينشأ من تسابق بين معالجة SYN cookies وتجزئة المقابس. ويستطيع مهاجم عن بُعد دون مصادقة إرسال حزم TCP مصممة لإحداث انهيار في النواة وإسقاط الخادم.

الأثر وحدوده

الأثر يقتصر على التوافر. وبحسب المصدر لا تتيح الثغرة تعديل البيانات ولا تنفيذ شيفرة عشوائية. نافذة التسابق ضيقة، وقد يستغرق النجاح على خادم فعلي هادئ وقتًا طويلاً. ويتطلب الاستغلال توزيع معالجة الحزم بين سياقات مختلفة، وهو ما ينطبق على الخوادم ذات طابوري RX أو أكثر أو التي يوزّع فيها RPS الحزم على عدة معالجات.

المعالجة

التصحيح متاح، وقد دُمج الإصلاح في النواة الرئيسية قبل أسبوعين من تقرير المصدر. وإن تعذّر التحديث فورًا يقترح الباحث تعطيل SYN cookies، مع ما يعنيه من انخفاض الحماية من هجمات SYN flood، وحصر المعالجة في طابور RX واحد لمنع التسابق.

بالنسبة للجهات المنظِّمة، يتركز الاهتمام على توافر الخدمات المبنية على لينكس والمكشوفة للإنترنت. يُنصح بترتيب الأولويات للمضيفات المكشوفة وتقدير كلفة الحلول المؤقتة قبل تطبيقها.

ما يجب فعله الآن

1. حصر خوادم لينكس التي تستقبل حركة TCP مباشرة، وخاصة التي تشغّل Nginx أو Apache أو SSH.
2. الحصول على تحديث النواة من مزوّد التوزيعة وجدولة التصحيح مع إعطاء الأولوية للمضيفات المكشوفة للإنترنت.
3. عند تعذّر التصحيح الفوري، تقييم الحلين المؤقتين: تعطيل SYN cookies أو استخدام طابور RX واحد، وتوثيق ضعف الحماية من SYN flood كمخاطرة مقبولة.
4. مراجعة الجاهزية العالية والتحويل التلقائي للخدمات الحرجة كي لا يؤدي انهيار مضيف إلى انقطاع.
5. رصد حالات انهيار النواة أو إعادة التشغيل غير المفسَّرة على الخوادم المكشوفة وتصعيدها عبر إدارة الحوادث.