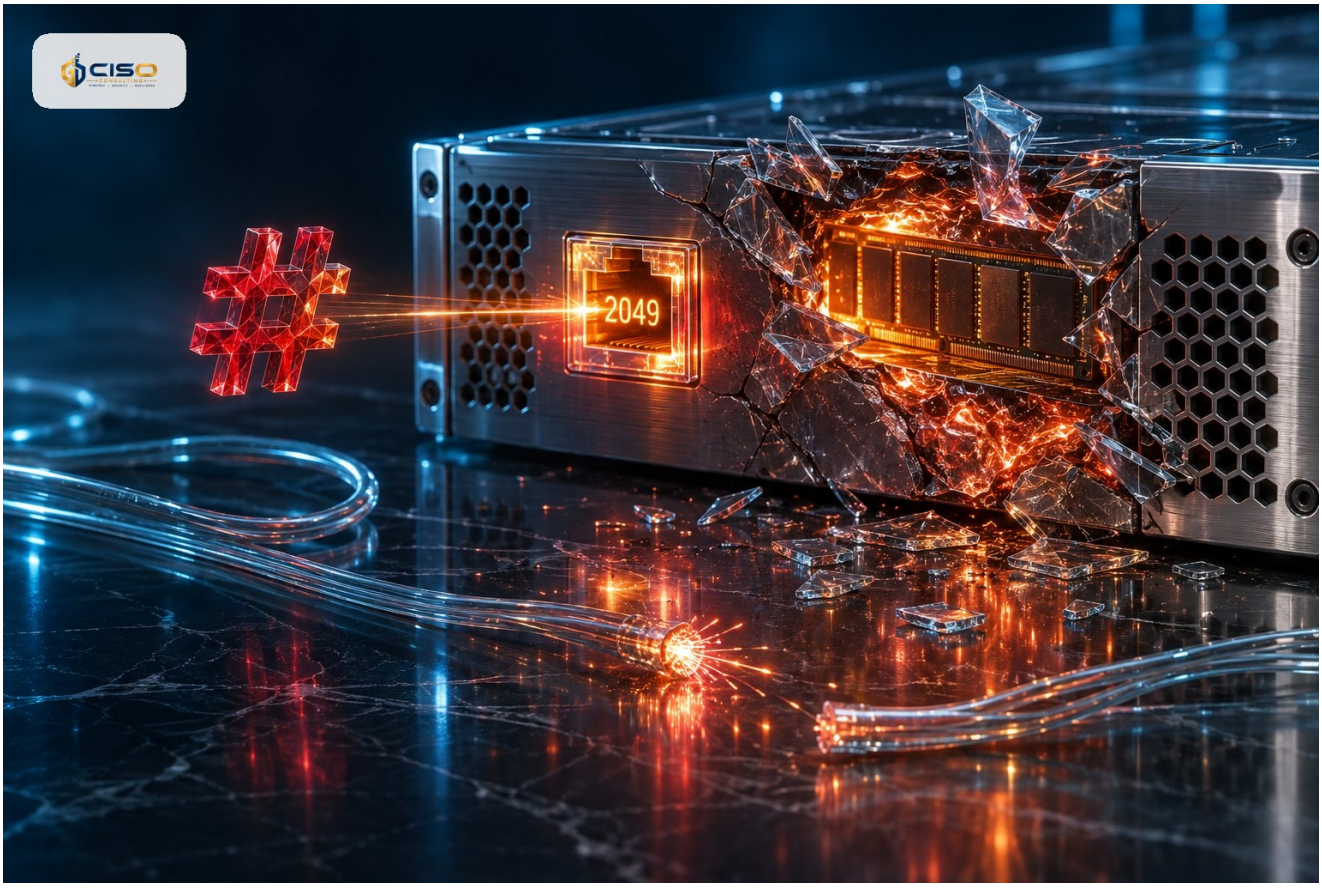
NFS2ROOT: ثغرة حرجة في خادم NFS على لينكس تتيح الحصول على صلاحيات الجذر عن بُعد



ثغرة حرجة (CVE-2026-99362) في خادم NFS بنواة لينكس تتيح لمهاجم عن بُعد الحصول على صلاحيات الجذر إذا كان nfsd يعمل والمنفذ 2049 متاحًا. ولم يُبلَّغ عن استغلال فعلي.

- الثغرة CVE-2026-99362 المسماة NFS2ROOT هي تجاوز سعة في الذاكرة الكومة (heap) داخل خادم nfsd (NFS) في نواة لينكس، وهي موجودة منذ الإصدار 3.16.
- تشمل الأنظمة ذات النواة الأقدم من 6.12.117 أو 6.18.61 أو 7.3.2 أو 7.4-rc1 عند تشغيل nfsd (الإصدار 4.1 أو 4.2) وإتاحة المنفذ TCP 2049 عبر الإنترنت.
- الهجوم منخفض التعقيد ولا يحتاج صلاحيات أو تفاعل مستخدم، ويمكنه تجاوز KASLR وتنفيذ أوامر بصلاحيات الجذر.
- لا توجد تقارير عن استغلال فعلي، لكن OpenSec شاركت استغلالاً كاملاً وتصحيحًا مع مشرفي NFSD.

- التخفيف: التحديث وإعادة التشغيل، أو حصر المنفذ 2049 بالجهات الموثوقة، أو تعطيل nfs-server عند عدم الحاجة.

تتيح ثغرة حرجة في خادم NFS بنواة لينكس، تحمل الرقم CVE-2026-99362 وسُميت NFS2ROOT، لمهاجم عن بُعد بلا أي صلاحيات أن يسيطر على الخادم بصلاحيات الجذر. اكتشفها Jérémy Jean من ANSSI وقدّم إصلاحًا في أغسطس، فيما شاركت شركة OpenSec استغلالاً كاملاً وتصحيحًا مع مشرفي NFSD في أواخر سبتمبر.

الأنظمة المتأثرة

الثغرة تجاوز سعة في الذاكرة (heap buffer overflow) داخل nfsd، وهي موجودة منذ النواة 3.16 الصادرة في مارس 2014. يكون النظام معرضًا إذا كانت نواته أقدم من 6.12.117 أو 6.18.61 أو 7.3.2 أو 7.4-rc1، وكان nfsd (الإصدار 4.1 أو 4.2) محمّلاً وقيد التشغيل، وكان المنفذ TCP 2049 متاحًا عبر الإنترنت.

يرسل المهاجم طلبات مصمَّمة تجعل الخادم يكتب خارج المخزن المخصص له، فيتمكن من قراءة ذاكرة النواة وتجاوز KASLR وزرع أمر تنفذه النواة بصلاحيات الجذر عند إغلاق الاتصال. لا يتطلب الهجوم تفاعل أي مستخدم. ولم ترد حتى الآن تقارير عن استغلال فعلي.

التخفيف والرصد

الخطوة الموصى بها هي تثبيت أحدث تحديث أمني للنواة من مزود التوزيعة ثم إعادة التشغيل لضمان تفعيل النواة المصححة. وإذا تعذّر التحديث فورًا فيُقصر الوصول إلى المنفذ 2049 على العملاء أو الشبكات الموثوقة، أو يُوقف ويُعطَّل نظام nfs-server إن لم تكن المشاركة عبر NFS مطلوبة.

وتشير OpenSec إلى أن الهجمات لا تترك توقيعات شبكية. ومن المؤشرات المحتملة: تحذيرات النواة الصادرة عن nfsd4_check_resp_size، وأوامر shell تبدأها عمليات النواة على خادم ملفات، ودفعات من جلسات NFSv4.1 قصيرة من مصدر واحد، وأعطال النواة (oops) التي تتضمن إطارات nfsd4_* أو svc_* أو call_usermodehelper*.

ما يجب فعله الآن

1. حصر خوادم لينكس وأجهزة NAS ومضيفات البناء وعقد التخزين في Kubernetes التي تشغّل nfsd، ومطابقة إصدارات النواة مع الإصدارات المصححة.
2. التحقق من إتاحة المنفذ TCP 2049 عبر الإنترنت، وإغلاقه أو حصره فورًا بالشبكات الموثوقة.
3. تثبيت تحديث النواة الأمني من المزود ثم إعادة التشغيل والتأكد من عمل النواة المصححة.
4. عند تأخر التحديث، تعطيل nfs-server على المضيفات التي لا تحتاج مشاركة NFS.
5. إضافة مؤشرات OpenSec (تحذيرات nfsd4_check_resp_size، وأوامر shell من عمليات النواة، ودفعات جلسات NFSv4.1 القصيرة) إلى الرصد ومراجعة السجلات الأخيرة.
6. توثيق التعرض والمعالجة ضمن إدارة الثغرات بما يخدم متطلبات الإبلاغ لدى الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي.