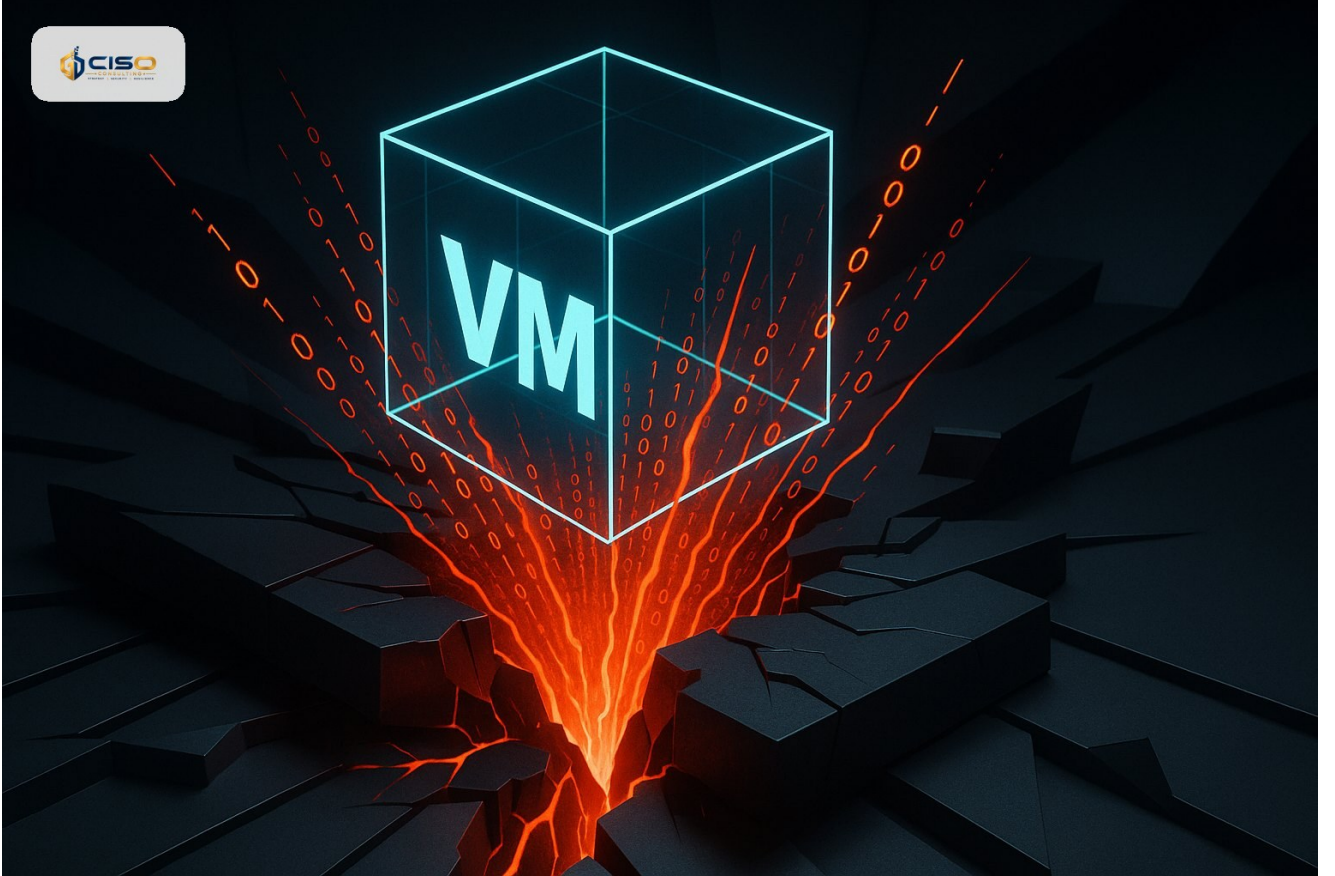


ثغرة PwnEscape الحرجة في نواة لينكس تمكّن الأجهزة الافتراضية الضيفة من قراءة ذاكرة المضيف



ثغرة حرجة في كود الشبكات بنواة لينكس تسمح للأجهزة الافتراضية بقراءة ذاكرة المضيف، مما يؤثر على البيانات السحابية التي تعتمد على المحاكاة الافتراضية لعزل المستأجرين.

- الثغرة CVE-2026-99999 المعروفة باسم PwnEscape هي خلل حرج في كود الشبكات بنواة لينكس يؤثر على بيانات المحاكاة الافتراضية
- تسمح الثغرة للكود العامل داخل جهاز افتراضي ضيف بقراءة ذاكرة نظام المضيف
- يكمن الخلل في النواة نفسها وليس في إعدادات مزودي الخدمات السحابية المحددة
- أثبت باحث وجود الثغرة على بيانات سحابية حية مع تأكيد من المزود
- تشكل المسألة خطراً كبيراً على البيانات السحابية متعددة المستأجرين التي تعتمد على عزل الأجهزة الافتراضية

نظرة عامة على الثغرة

تم الكشف عن ثغرة أمنية حرجية تحمل الرمز **CVE-2026-99999** واسم **PwnEscape** في نواة لينكس. توجد الثغرة في كود الشبكات الخاص بالنواة وتمكّن الكود الذي يعمل داخل جهاز افتراضي ضيف من قراءة الذاكرة التابعة لنظام المضيف. أثبت باحث أمني وجود الثغرة على بيانات سحابية حية، وأكد المزود المتأثر الثغرة.

النطاق والأثر

على عكس نقاط الضعف في الإعدادات الخاصة بمزودي الخدمات السحابية الفرديين، تكمن ثغرة PwnEscape في نواة لينكس نفسها، مما يعني أن الثغرة تؤثر على الطبقة الأساسية المشتركة عبر منصات المحاكاة الافتراضية. يشكل هذا تهديداً كبيراً للبيئات السحابية متعددة المستأجرين حيث يعد العزل بين الأجهزة الافتراضية الضيفة والمضيف أمراً ضرورياً للأمن. قد تؤدي القدرة على قراءة ذاكرة المضيف إلى كشف بيانات حساسة وبيانات اعتماد ومفاتيح تشفير ومعلومات تخص مستأجرين آخرين يتشاركون نفس البنية التحتية المادية.

التداعيات على المؤسسات الخاضعة للتنظيم

بالنسبة للمؤسسات في المملكة التي تشغل بنية تحتية افتراضية أو تستهلك خدمات سحابية، تمثل هذه الثغرة خطراً مادياً على سرية البيانات وضوابط عزل المستأجرين. يجب على الجهات الخاضعة للتنظيم التي تعتمد على المحاكاة الافتراضية لفصل أحمال العمل تقييم مدى تعرضها والتنسيق مع مزودي البنية التحتية والخدمات السحابية لفهم الجداول الزمنية للترقيع والضوابط التعويضية خلال فترة المعالجة.

ما يجب فعله الآن

1. جرد جميع البنية التحتية الافتراضية والخدمات السحابية المستخدمة وتحديد تلك التي تعمل على أنظمة مضيضة أو hypervisors قائمة على لينكس
2. التواصل مع مزودي البنية التحتية والخدمات السحابية لتأكيد التعرض للثغرة CVE-2026-99999 والحصول على جداول الترقيع
3. مراجعة ضوابط عزل المستأجرين وتقييم ما إذا كانت أحمال العمل الحساسة تتشارك مضيفات مادية مع بيانات غير موثوقة أو ذات تصنيف أقل
4. تطبيق تجزئة شبكية إضافية ومراقبة لحركة المرور الأفقية بين الأجهزة الافتراضية وأنظمة المضيف حيثما أمكن
5. إعطاء الأولوية لترقيع أنظمة hypervisors لينكس الداخلية فور توفر تحديثات المزودين
6. توثيق الثغرة في سجلات المخاطر وإبلاغ لجان الحوكمة بالتعرض المحتمل خلال فترة المعالجة