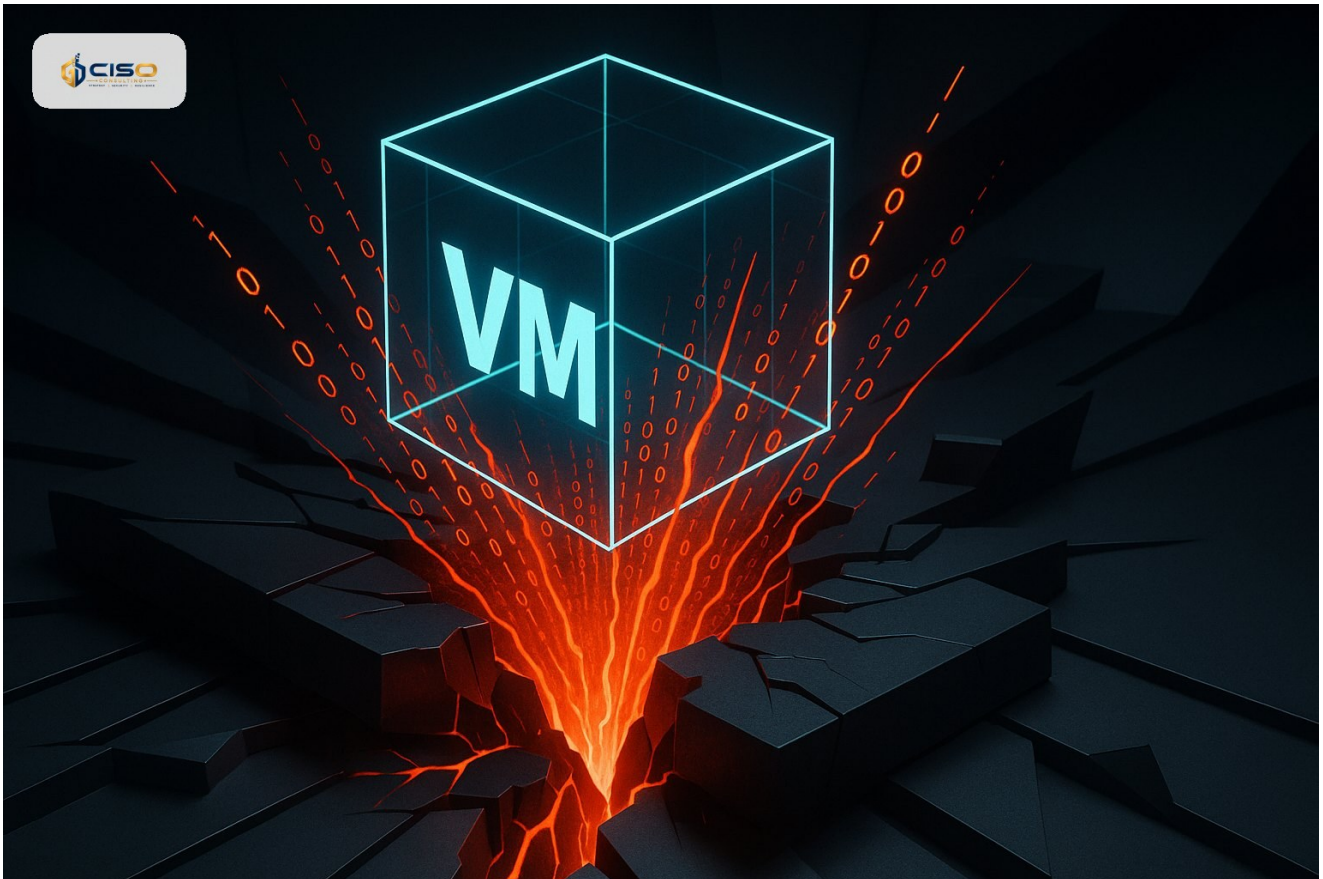


Critical Linux kernel flaw PwnEscape enables guest VMs to read host memory



A critical vulnerability in the Linux kernel networking code allows virtual machines to read host memory, affecting cloud environments relying on virtualisation for tenant isolation.

- CVE-2026-99999 (PwnEscape) is a critical flaw in the Linux kernel networking code affecting virtualisation environments
- The vulnerability allows code running inside a guest virtual machine to read memory on the host system
- The flaw resides in the kernel itself, not in specific cloud provider configurations
- A researcher demonstrated the vulnerability against live cloud sandboxes, with vendor confirmation
- The issue poses a significant risk to multi-tenant cloud environments relying on VM isolation

Vulnerability overview

A critical security flaw tracked as **CVE-2026-99999** and nicknamed **PwnEscape** has been disclosed in the Linux kernel. The vulnerability exists in the kernel's networking code and enables code executing inside a guest virtual machine to read memory belonging to the host system. A security researcher demonstrated the flaw against live cloud sandbox environments, and the affected vendor confirmed the vulnerability.

Scope and impact

Unlike configuration weaknesses specific to individual cloud providers, PwnEscape resides in the Linux kernel itself, meaning the vulnerability affects the foundational layer shared across virtualisation platforms. This poses a significant threat to multi-tenant cloud environments where isolation between guest VMs and the host is essential for security. The ability to read host memory could expose sensitive data, credentials, encryption keys, and information belonging to other tenants sharing the same physical infrastructure.

Implications for regulated institutions

For organisations in the Kingdom operating virtualised infrastructure or consuming cloud services, this vulnerability represents a material risk to data confidentiality and tenant isolation controls. Regulated entities relying on virtualisation for workload separation must assess their exposure and coordinate with infrastructure and cloud service providers to understand patching timelines and compensating controls during the remediation window.

What to do now

1. Inventory all virtualised infrastructure and cloud services in use, identifying those running Linux-based hypervisors or host systems
2. Contact infrastructure and cloud service providers to confirm exposure to CVE-2026-99999 and obtain patching schedules
3. Review tenant isolation controls and assess whether sensitive workloads share physical hosts with untrusted or lower-classification environments
4. Implement additional network segmentation and monitoring for east-west traffic between VMs and host systems where feasible
5. Prioritise patching of on-premises Linux hypervisors once vendor updates become available
6. Document the vulnerability in risk registers and inform governance committees of potential exposure during the remediation period