

CVE-2025-39964: Linux kernel race condition in AF_ALG sockets



CISA lists CVE-2025-39964, a Linux kernel race condition where concurrent writes to one AF_ALG socket can interleave data and corrupt internal state. Apply vendor mitigations and assess internet exposure.

- CVE-2025-39964 is a race condition in the Linux kernel.
- Concurrent writes to the same AF_ALG socket can interleave data unpredictably.
- The result is inconsistency in the socket's internal state.
- CISA requires vendor mitigations under BOD 26-04 and its forensics triage requirements.
- The CISA federal due date is 2026-09-21; stakeholders must assess each asset's internet exposure.

What was disclosed

CISA has listed CVE-2025-39964, a race condition in the Linux kernel. When several writes happen at the same time on a single AF_ALG socket, the data can be interleaved in an unpredictable way. This leaves the socket's internal state inconsistent.

The source does not describe a specific exploitation scenario, affected kernel versions or the impact beyond this inconsistency, so teams should rely on their Linux distribution or vendor for exact version guidance.

What CISA requires

CISA's required action is to apply mitigations according to vendor instructions, in line with its BOD 26-04 guidance on prioritizing security updates based on risk and its Forensics Triage Requirements. Where a cloud service is involved, the applicable BOD 26-04 guidance should be followed. If mitigations are not available, the product should no longer be used. The federal due date is 2026-09-21.

Stakeholders are responsible for judging the internet exposure of each asset and for keeping to the BOD 26-04 patching guidelines.

Practical view for Saudi institutions

The CISA deadline applies to US federal bodies, but it is a useful benchmark for prioritization. Linux is widespread across servers, appliances and cloud workloads, so the first task is knowing where it runs and which assets are reachable from the internet. Patch those first, record the decisions taken, and keep the evidence for audit.

What to do now

1. Inventory Linux hosts, appliances and cloud workloads and map which are internet-exposed.
2. Check your Linux vendor's advisories for CVE-2025-39964 and apply the supplied mitigations or kernel updates.
3. Prioritize internet-facing assets, using CISA's September 21, 2026 date as a planning benchmark.
4. Where no mitigation exists for a product, plan its replacement or retirement.
5. Document patch decisions and exceptions as evidence for NCA ECC and SAMA CSF reviews.