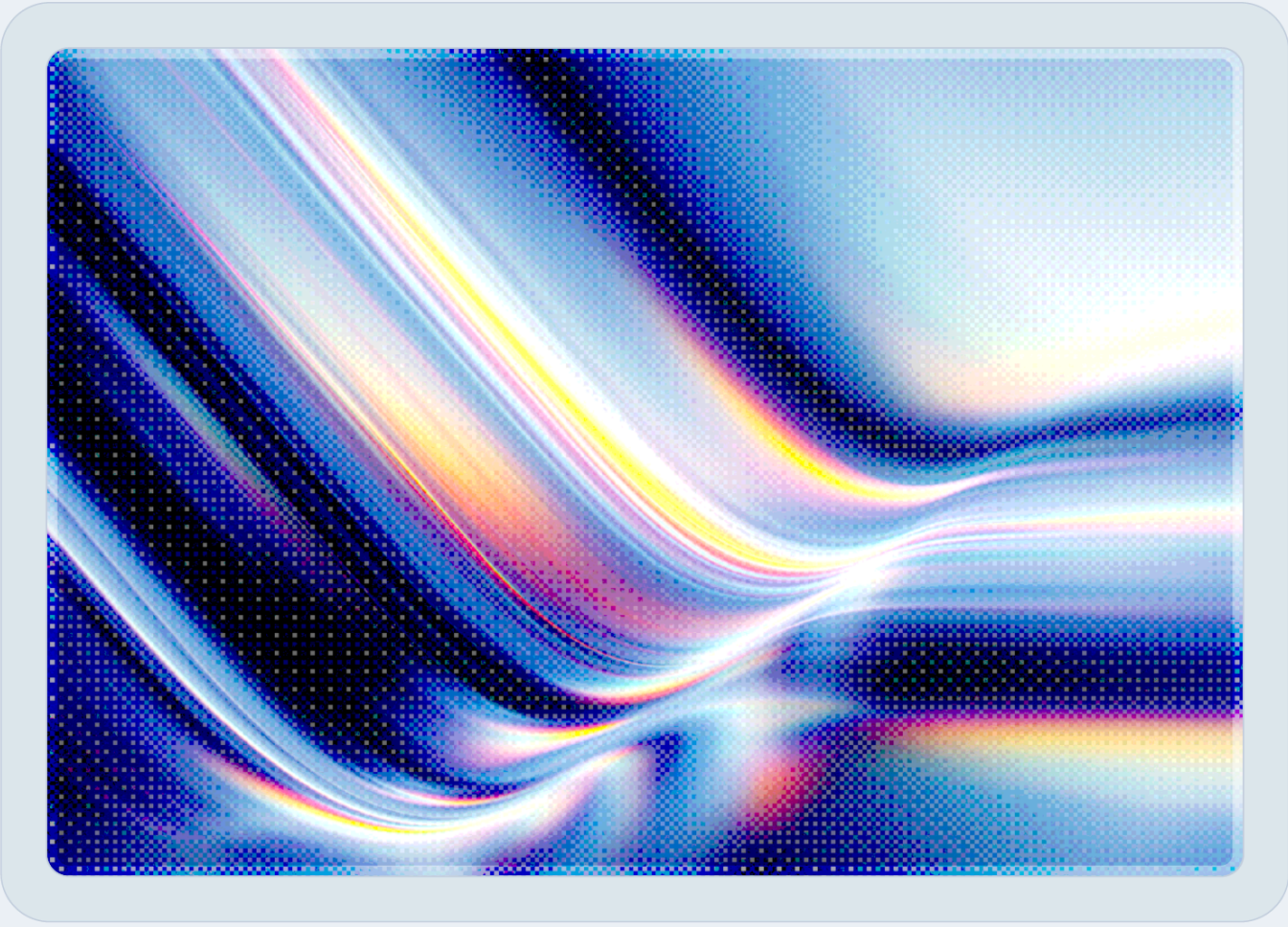
CSAI Foundation | Cloud Security Alliance

CISA Flags Three Actively Exploited Linux Kernel Flaws

2026-09-23

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

On September 18, 2026, the Cybersecurity and Infrastructure Security Agency (CISA) added three Linux kernel vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog after confirming evidence of active exploitation, giving Federal Civilian Executive Branch agencies until September 21 to remediate under Binding Operational Directive (BOD) 26-04 [1][2][3]. The three flaws sit in unrelated kernel subsystems, a race condition in the AF_ALG cryptographic socket interface (CVE-2025-39964), an out-of-bounds write in the ebtables SNAT netfilter target (CVE-2026-53266), and a logic error in the kernel TLS receive path (CVE-2025-39682); their simultaneous addition to the catalog may reflect independent discovery across unrelated subsystems rather than a single coordinated campaign, though CISA has not disclosed enough detail to confirm or rule out a shared attack chain [1][2]. Red Hat has confirmed working public exploits for all three vulnerabilities and rated each a high-priority remediation item, while CISA has disclosed no details of the specific intrusions that triggered the KEV listing beyond requiring covered agencies to perform forensic triage of potentially affected assets rather than treating a patch as sufficient closure [2][4]. The AF_ALG flaw is notable for its age, a defect present in the kernel's cryptographic user API for roughly fourteen years before STAR Labs researchers were credited with its discovery; public reporting to date has not detailed the specific exploitation technique or confirmed container-escape impact beyond the vulnerability's documented denial-of-service and integrity-failure potential [5][6]. None of the three vulnerabilities has so far been linked to ransomware operations [2][3]. CSA recommends that organizations outside the federal civilian enterprise nonetheless treat the September 21 deadline as a floor rather than a benchmark, since BOD 26-04 governs only agencies directly covered by the directive.

Background

The Linux kernel has been the subject of a steady stream of high-severity, publicly exploited vulnerability disclosures in 2026, a trend CSA has tracked across a series of rapid-research advisories [7][8]. The three vulnerabilities CISA added to the KEV catalog on September 18 extend that pattern into the traffic-control, cryptographic, and networking layers of the kernel rather than repeating the page-cache and container-escape themes that dominated the spring 2026 disclosures. CVE-2025-39682 and CVE-

2025-39964 were assigned CVE identifiers in 2025, meaning the underlying code defects predate this year's exploitation activity by a meaningful margin and were only recently confirmed as actively targeted; CVE-2026-53266 is a 2026 identifier tied to more recent ebtables research [1][2].

CISA's KEV catalog exists to translate the full range of disclosed vulnerabilities into a prioritized, evidence-based list that Federal Civilian Executive Branch agencies are bound to act on under Binding Operational Directive 26-04, which replaced the agency's earlier BOD 22-01 remediation framework with a risk-tiered model that can compress patch timelines to as little as three calendar days for the highest-risk entries [3][9]. All three Linux kernel vulnerabilities received that compressed timeline: CISA published the KEV additions on September 18 and set the remediation deadline for September 21, a three-day window that BOD 26-04's risk matrix assigns when a vulnerability is publicly exploited, has an automatable exploit, and produces total control impact, criteria all three vulnerabilities appear to satisfy [1][2][3][10]. Red Hat's own advisories, updated in the early hours of September 19 UTC, independently corroborated the exploitation assessment, stating for at least one of the three CVEs that "this CVE is high risk and there are known public exploits leveraging this vulnerability" and urging customers to "address this vulnerability with high priority" [1].

This research note builds on CSA's September 20, 2026 initial alert on this KEV addition, "CISA's 72-Hour Window for Three Linux Kernel Flaws" [11], incorporating additional source verification and refining several claims from that earlier alert that follow-on reporting did not fully support. It summarizes what is publicly known about each of the three vulnerabilities, situates the KEV listing within CISA's broader directive framework, and provides remediation guidance for security and infrastructure teams managing Linux fleets, whether or not their organization falls under BOD 26-04's direct authority.

Security Analysis

CVE-2025-39682: TLS receive-path logic error

CVE-2025-39682 carries the highest severity of the three, with a CVSS base score of 9.8, and lies in the kernel's handling of the transport layer security receive path when kernel TLS (kTLS) offload is in use [2][4]. The flaw stems from an assumption in the kernel's `recvmsg()` logic that no record-type transitions occur after zero-copy decryption completes; that assumption breaks when a zero-length TLS record queued on the socket's `rx_list` is processed alongside records of a different type, allowing different TLS record types to be handled together in ways the receive path was not designed to tolerate [4]. The practical impact ranges from denial of service to memory disclosure, and Red Hat has confirmed that public exploits for the flaw are available, which is consistent with CISA's decision to compress the federal remediation window to three days [1][4].

CVE-2026-53266: ebtables SNAT out-of-bounds write

CVE-2026-53266, rated 8.8 on the CVSS scale, affects the bridge netfilter subsystem's ebtables SNAT target when it is configured to rewrite the ARP sender hardware address on packets crossing a bridge interface [2][4]. During that optional rewrite, the kernel can call `skb_store_bits()` without first confirming that the destination memory range is writable; when the affected data resides in a nonlinear socket-buffer fragment backed by a splice-imported file page, the write lands directly in the underlying page rather than in a private buffer, producing memory corruption [12]. Triggering the flaw requires local access: an attacker needs the CAP_NET_ADMIN capability to configure the ebtables rule and craft the ARP packet that traverses the affected bridge, rather than mere network adjacency [12]. Kernel maintainers have shipped an upstream fix and backported it to the 5.10.259, 6.1.176, and 6.12.94 stable branches, and Red Hat has confirmed a working exploit exists for the flaw [2][4]. Organizations that cannot patch immediately can disable ARP hardware-address rewriting in their ebtables SNAT rules, or remove ebtables SNAT rules that operate on ARP traffic on bridge interfaces, as an interim compensating control [2][4].

CVE-2025-39964: a fourteen-year-old race condition in AF_ALG

CVE-2025-39964, scored 7.8, is a race condition in the AF_ALG cryptographic socket interface that has existed in the kernel for approximately fourteen years [1][5]. The defect allows two concurrent writers to issue data to the same AF_ALG socket, interleaving request payloads unpredictably and leaving the socket's internal per-connection state inconsistent; depending on how an application relies on that socket's cryptographic output, the result can range from a system crash to silently corrupted cryptographic operations, either of which constitutes a denial-of-service or data-integrity failure [1][5]. STAR Labs SG researchers are credited with discovering the flaw. Public reporting to date has not detailed the specific exploitation technique or confirmed container-escape impact beyond the vulnerability's documented denial-of-service and integrity-failure potential; CISA and Red Hat have confirmed only that the flaw is being exploited in the wild and that public exploits exist, not the outcome those exploits achieve [5][6]. A public proof-of-concept exploit for the vulnerability is available on GitHub, further narrowing the gap between disclosure and any attacker's ability to weaponize it [6].

A shared response, not a shared root cause

Table 1 summarizes the three vulnerabilities side by side. The pattern that unites them is not a common code defect but a common institutional response: CISA's evidence-based confirmation of active exploitation, Red Hat's independent corroboration through its own customer advisories, and a

compressed remediation clock under BOD 26-04 that treats confirmed in-the-wild exploitation, rather than CVSS severity alone, as the trigger for urgency [1][2][3].

CVE	CVSS	Kernel subsystem	Primary impact	Age at disclosure
CVE-2025-39682	9.8	TLS receive path (kTLS)	DoS, memory disclosure	Recent
CVE-2026-53266	8.8	Bridge netfilter (ebtables SNAT)	Memory corruption, DoS, possible privilege escalation	Recent
CVE-2025-39964	7.8	AF_ALG crypto socket API	System crash, cryptographic integrity failure	~14 years

CISA's requirement that covered agencies perform forensic triage, rather than treat successful patch deployment alone as sufficient, reflects an operating assumption that some affected assets may already have been exploited before the KEV listing and directive deadline existed [2]. That posture is a meaningful departure from routine patch-management guidance and should inform how security teams, federal or otherwise, scope their own response to these three vulnerabilities.

Recommendations

Immediate Actions

Security and infrastructure teams should inventory every Linux host, container, and virtual machine against the kernel versions that resolve CVE-2025-39682, CVE-2026-53266, and CVE-2025-39964, prioritizing internet-facing systems, multi-tenant hosts, and any system that terminates TLS in-kernel or processes bridged network traffic with ebtables rules configured, since those configurations are directly implicated in the TLS and ebtables flaws respectively [1][2][4]. Teams supporting Federal Civilian Executive Branch agencies must complete remediation and the forensic triage CISA has mandated by the directive's deadline; teams outside that scope should nonetheless treat the September 21 date as the point at which public exploit availability for all three vulnerabilities should be assumed to be mature

[2][3]. Where immediate kernel patching is not feasible for the ebtables flaw, disabling ARP hardware-address rewriting in ebtables SNAT rules, or removing SNAT rules that act on ARP traffic on bridge interfaces, closes the specific exploitation path without requiring a kernel update [2][4].

Short-Term Mitigations

Because CVE-2025-39964's discovery is credited to researchers who reported exploitation well beyond a theoretical denial-of-service scenario, organizations running shared or multi-tenant Linux hosts, including containerized AI and machine learning infrastructure, should treat a delayed patch for that flaw as a potential isolation risk and not merely a local denial-of-service concern, consistent with the pattern CSA has documented in other 2026 Linux kernel local privilege escalation research, even though the specific exploitation technique remains undetailed in public reporting [5][7][8]. Teams that cannot patch all three vulnerabilities within the federal window should sequence remediation by exploit maturity and blast radius: CVE-2025-39964's published proof-of-concept exploit and long exposure window argue for treating it as at least as urgent as its 7.8 CVSS score alone would suggest [5][6]. Detection teams should extend monitoring beyond kernel version inventories to include forensic review of systems that were internet-exposed or running affected configurations prior to the September 18 KEV addition, mirroring CISA's own triage requirement even for organizations outside the directive's direct authority [2].

Strategic Considerations

The recurrence of high-severity, actively exploited Linux kernel vulnerabilities across unrelated subsystems in 2026, from page-cache corruption and futex use-after-free flaws earlier in the year to this September's TLS, netfilter, and cryptographic-socket disclosures, indicates that kernel-level vulnerability management deserves the same prioritization discipline security teams already apply to internet-facing application vulnerabilities [7][8]. Organizations should evaluate whether their existing patch-management SLAs can support a three-day remediation window when CISA's risk-tiering under BOD 26-04 calls for one, and whether their asset inventory is granular enough to identify which hosts run the specific kernel configurations, such as kTLS offload or ebtables ARP rewriting, that these vulnerabilities require [3][4]. For organizations that do not fall under BOD 26-04, the directive's risk-tiered approach nonetheless offers a useful external benchmark: the three-day tier reflects BOD 26-04's own published criteria for publicly exploited, automatable, total-control-impact vulnerabilities, and internal vulnerability management programs can reasonably calibrate their own urgency against that same published risk matrix even without a regulatory obligation to do so [3][10].

CSA Resource Alignment

This advisory extends a pattern CSA's AI Safety Initiative has tracked through several 2026 Linux kernel research notes. "GhostLock: 15-Year-Old Linux Kernel Flaw Grants Root, Escapes Containers" examined a futex use-after-free vulnerability, CVE-2026-43499, that had also gone undetected in the kernel for roughly fifteen years before public exploitation, a near-identical age profile to CVE-2025-39964's fourteen-year exposure window documented in this note, and its remediation guidance on host-kernel patching discipline and container-isolation limits applies directly to organizations assessing how urgently to close CVE-2025-39964's long-lived exposure window [7]. "Dirty Frag: Linux Kernel LPE Threatens Cloud AI Infrastructure" analyzed a separate chained local privilege escalation affecting Linux hosts running AI and machine learning workloads, and its emphasis on the outsized consequences of kernel compromise on shared GPU and inference infrastructure is directly relevant to any organization deciding how to sequence patching across the three vulnerabilities covered here when multi-tenant AI infrastructure is in scope [8]. "CISA BOD 26-04: AI Threat Forces 3-Day Critical Patch Mandate" details the directive's four-factor risk matrix, asset exposure, KEV status, exploit automation, and technical impact, that produces the compressed remediation tiers discussed throughout this note, and readers seeking the full mechanics behind the three-day deadline should consult it directly [10]. Finally, the AI Controls Matrix (AICM) v1.1, CSA's control framework for cloud and AI environments, provides the Threat and Vulnerability Management and Infrastructure Security domain controls that translate this note's immediate-action and short-term-mitigation guidance, including asset inventory, patch prioritization, and compensating controls for infrastructure supporting AI workloads, into auditable requirements applicable across the model-provider, application-provider, and cloud-service-provider roles [13].

References

[1] The Hacker News. "CISA Flags Three Linux Kernel Vulnerabilities Exploited in the Wild." The Hacker News, September 2026.

[2] BleepingComputer. "CISA alerts of active exploitation of three Linux kernel flaws." BleepingComputer, September 2026.

[3] Cybersecurity and Infrastructure Security Agency. "Binding Operational Directive 26-04: Prioritizing Security Updates Based on Risk." CISA, 2026.

[4] SecurityWeek. "Organizations Warned of 3 Exploited Linux Kernel Vulnerabilities." SecurityWeek, September 2026.

[5] LinuxSecurity. "CISA Alerts on Ongoing Exploitation of Linux Kernel Crypto Vulnerability." LinuxSecurity, September 2026.

[6] Suominen, Kimmo. "CVE-2025-39964 Proof of Concept." GitHub, 2026.

[7] Cloud Security Alliance. "GhostLock: 15-Year-Old Linux Kernel Flaw Grants Root, Escapes Containers." CSA AI Safety Initiative, July 14, 2026.

[8] Cloud Security Alliance. "Dirty Frag: Linux Kernel LPE Threatens Cloud AI Infrastructure." CSA AI Safety Initiative, May 13, 2026.

[9] Cybersecurity and Infrastructure Security Agency. "Known Exploited Vulnerabilities Catalog." CISA, 2026.

[10] Cloud Security Alliance. "CISA BOD 26-04: AI Threat Forces 3-Day Critical Patch Mandate." CSA AI Safety Initiative, June 13, 2026.

[11] Cloud Security Alliance. "CISA's 72-Hour Window for Three Linux Kernel Flaws." CSA AI Safety Initiative, September 20, 2026.

[12] SentinelOne. "CVE-2026-53266: Linux Kernel Privilege Escalation Flaw." SentinelOne Vulnerability Database, 2026.

[13] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2026.

