Week commencing 23 November 2026

ClearPath Partnership

COVERAGE
9 – 22 November 2026

AUDIENCE
Technology and security leadership · platform and delivery leads

HANDLING
Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING…

AI inference and gateway software now has its own line in the exploited-vulnerability catalogue.

CISA added GPUStack, an AI model-serving platform, and LiteLLM, a widely used LLM gateway, to its exploited-vulnerability catalogue twice in one fortnight — one attack used a malicious inference backend to open a reverse shell. Ask this week: which AI inference servers and gateways do we actually run, and are they patched on the same cycle as everything else internet-facing.

THIS FORTNIGHT

Platform change and AI regulation

PRIORITY

9–18 NOV

AI inference and gateway tools join the exploited-vulnerability catalogue

CISA added GPUStack to the KEV catalogue on 9 November after attackers used a malicious inference backend to open a reverse shell; the patch deadline has already passed. On 18 November it added BerriAI's LiteLLM gateway (CVE-2026-40217), for which proof-of-concept code is public, with a 2 December deadline.

So what: inventory every AI inference server and LLM gateway you run, in or out of production — these are now routine exploitation targets, not pilot infrastructure.

PRIORITY

10 NOV

November Patch Tuesday: exploited Outlook zero-day, critical Exchange flaw

Microsoft's 10 November update fixed an exploited Outlook spoofing flaw, CVE-2026-124194, which can be relayed or cracked to recover a user's credentials; CISA set a 24 November KEV deadline. The same release carries CVE-2026-118207, a critical Exchange Server flaw rated 8.8, flagged for emergency patching.

So what: patch Outlook and Exchange Server before Tuesday's KEV deadline — Exchange sits ahead of every mailbox in your estate.

PRIORITY

2–9 NOV

Copilot Chat limits land for unlicensed users; billing date slips to December

Microsoft began capping Copilot Chat for users without a paid licence — 2 November for tenants under 2,000 seats, 9 November for larger ones — on limits admins cannot view or adjust. Usage-based billing for new Copilot Business purchases, originally due 2 November, now starts 1 December.

So what: budget for metered AI costs from December, and tell unlicensed staff their Copilot Chat access is about to shrink.

WATCH

MID-NOV

Entra ID defaults to CAPTCHA on SMS and voice MFA

From mid-November, Entra ID applies risk-based CAPTCHA verification before some users receive an SMS code or voice call for MFA. It lands alongside the agent-blueprint-creation rollout begun 4 November, which continues through late November and still needs an explicit admin opt-out.

So what: brief the service desk before the CAPTCHA calls start, and confirm agent-blueprint creation is disabled if you haven't already.

ACTION QUEUE

Changes to act on this fortnight

CHANGE	PLATFORM	WHAT IT BREAKS OR REQUIRES	ACT BY
Outlook zero-day CVE-2026-124194	Microsoft 365	Exploited; can be relayed to recover a user's credentials.	24 Nov 2026
Exchange Server flaw CVE-2026-118207	Microsoft Exchange	Critical (8.8); emergency patch for every on-prem server.	Immediate
GPUStack exploitation, CVE-2026-102895	AI inference infra	Reverse shell via malicious inference backend; check for rogue admin keys.	Immediate
LiteLLM gateway flaw, CVE-2026-40217	AI gateway infra	Public exploit code; patch or isolate internet-facing gateways.	2 Dec 2026
Entra ID CAPTCHA on SMS/voice MFA	Microsoft Entra ID	Some users face a CAPTCHA step before receiving a code or call.	Rolling, mid-Nov

Dates and CVE identifiers as published by CISA and Microsoft; several Copilot billing dates have already moved twice this year.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- Entra ID agent-blueprint creation is open to every user by default since 4 November; admins must act to restrict it.
- Entra ID CAPTCHA for SMS/voice MFA and Copilot Chat limits for unlicensed users are both rolling out now.

Approaching

- LiteLLM KEV remediation deadline, 2 December 2026.
- Copilot usage-based billing for new Business purchases, now set for 1 December 2026.

Standing watch — sovereign cloud and data residency. No material change this fortnight; Azure Local's sovereign-scale expansion continues with no new published date.

AWS and Google Cloud: a quiet fortnight for both — nothing met the inclusion bar. AWS re:Invent (30 Nov–4 Dec) is the next date to watch.

RECOMMENDED

Three things to do before the next edition

- Inventory every AI inference server and LLM gateway in your estate, and patch or isolate GPUStack and LiteLLM now.
- Patch Outlook and Exchange Server before the 24 November KEV deadline passes.
- Confirm agent-blueprint creation is disabled and brief the helpdesk on the new MFA CAPTCHA step.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely further AI inference or gateway products are added to the KEV catalogue before the next edition, and a realistic possibility Microsoft confirms final Copilot Credit pricing. Expect AWS and Google Cloud announcements to pick up around re:Invent.

NEXT EDITION

Monday 7 December 2026. Send additions, corrections or platform intelligence to your ClearPath engagement lead.

ClearPath Partnership