Week commencing 14 September 2026

ClearPath Partnership

COVERAGE
31 August – 13 September 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…

Your AI gateway just became a confirmed target, not a theoretical one.

CISA's 2 September update included the first AI-infrastructure flaw it has ever listed as exploited: an authentication bypass in LiteLLM's MCP gateway, chained with a second bug to steal provider keys and mine cryptocurrency inside production AI proxies. Ask this week: does our AI gateway sit behind the same network controls as every other production system, or did it go in unreviewed?

THIS FORTNIGHT

Platform change and AI regulation

PRIORITY

2 SEP

First AI-infrastructure flaw lands in CISA's exploited-vulnerability catalogue

CISA added a LiteLLM MCP authentication-bypass flaw (CVE-2026-59822) to its exploited-vulnerabilities catalogue on 2 September, one of seven added that day. Attackers chained it with a Starlette smuggling bug to reach unauthenticated MCP endpoints, harvest provider keys, and deploy cryptocurrency miners inside production gateways.

So what: any self-hosted AI gateway or MCP proxy is now a confirmed target. Patch LiteLLM to 1.84.0 and review who has network access to it.

PRIORITY

8 SEP

Record Patch Tuesday ships two exploited Windows zero-days

Microsoft's September update fixed 974 vulnerabilities, its largest release on record, including two zero-days already under active exploitation: a Windows Update Stack privilege-escalation flaw (CVE-2026-81963) and an ALPC heap overflow (CVE-2026-85880), both granting SYSTEM-level access.

So what: triage the two exploited flaws ahead of the remaining 972 fixes; volume is a scheduling problem, active exploitation is not.

PRIORITY

6-8 SEP

Maximum-severity N-central flaw hands attackers every managed endpoint at once

N-able confirmed pre-disclosure exploitation of a pre-authentication remote-code-execution flaw in N-central (CVE-2026-86218, CVSS 10.0), its remote monitoring platform. A hotfix shipped 6 September; CISA catalogued the flaw two days later. Chained with two auth-bypass bugs, it lets attackers create administrator accounts outright.

So what: ask any managed service provider you use whether Hotfix 4 is applied — one compromised console reaches every endpoint it manages.

PRIORITY

SEP

EU AI Office opens its first compliance inspection wave

Following the 2 August high-risk deadline, the AI Office and national regulators — France's CNIL, Germany's BfDI, Spain's AESIA — began scheduled inspections this month, opening with automated CV-screening, algorithmic credit assessment and AI triage tools in private healthcare.

So what: if you deploy AI in EU recruitment, lending or healthcare triage, assume documentation requests are live now — check your Annex III conformity file is current.

ACTION QUEUE

Changes to act on this fortnight

CHANGE	PLATFORM	WHAT IT BREAKS OR REQUIRES	ACT BY
CVE-2026-59822 LiteLLM MCP bypass	AI gateway / MCP proxy	Unauthenticated MCP access; upstream provider keys exposed.	Immediate
CVE-2026-86218 N-central RCE	N-able RMM	Pre-auth takeover; attacker-created admin accounts across managed endpoints.	Immediate
CVE-2026-81963 / -85880	Microsoft Windows	SYSTEM-level compromise via update stack and ALPC; both exploited.	Immediate
CVE-2026-83548 / -83549 SMA1000	SonicWall remote access	SSRF and command injection, chainable to full appliance compromise.	Immediate
Passkeys become default sign-in	Microsoft Entra ID	SMS/voice users auto-enrolled and nudged — brief the helpdesk.	In effect since 1 Sep

Identifiers and dates as published by CISA, Microsoft and N-able. Confirm applicability against your own estate before scheduling.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- AI Act Annex III high-risk obligations apply since 2 August; the AI Office's first inspection wave is running through September.
- Entra ID SSPR accepts only pre-registered authentication methods, in force since 7 September.

Approaching

- Entra ID custom controls stop accepting new configurations this month and retire 30 September — migrate to External MFA.
- ICO's automated-decision-making guidance, consulted through May, is expected as a statutory code of practice later this year.

Standing watch — unmaintained AI gateway software. AWS archived its own Bedrock Access Gateway proxy on 4 September, the same week LiteLLM's gateway was added to KEV. Audit any self-hosted or community AI proxy for the same unmaintained-dependency risk.

RECOMMENDED

Three things to do before the next edition

- Patch LiteLLM to 1.84.0 and audit who can reach your MCP or AI gateway endpoints directly.
- Apply N-central Hotfix 4 or confirm your MSP has, then review admin accounts created since August.
- Prioritise September's two exploited Windows zero-days ahead of the remaining 972 patches.

OUTLOOK — NEXT FORTNIGHT

We assess it is highly likely further AI-infrastructure flaws reach KEV before the next edition, as gateways and MCP proxies get the scrutiny edge appliances did in 2025. It is a realistic possibility the AI Office issues its first EU AI Act enforcement action from this inspection wave, and likely that N-central sees follow-on exploitation among unpatched managed service providers.

NEXT EDITION

Monday 28 September 2026. Send additions, corrections or platform intelligence to your ClearPath engagement lead.

ClearPath Partnership