Week commencing 17 August 2026

ClearPath Partnership

COVERAGE
3 – 16 August 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…

Three separate agent platforms let attackers trigger tools without the model ever being called.

AWS Bedrock AgentCore, Google's Agent Development Kit and Vercel's coding-agent SDKs all shipped a way for a forged tool-call to reach a live tool directly, skipping the model and every guardrail attached to it. All three are now patched. Ask your AI platform owner today which production agents call tools through a harness rather than a model turn, and confirm each one has the fix.

THIS FORTNIGHT

Platform change and AI regulation

PRIORITY

6 AUG

Agent harnesses let tools fire without the model in the loop

AWS Bedrock AgentCore, Google's Agent Development Kit (CVE-2026-18236, CVSS 9.3) and Vercel's Codex and OpenCode SDKs each let a forged tool-call reach a host tool directly. Google separately deleted three ADK workflow templates on 4 August after a malicious GitHub issue triggered a privileged agent.

So what: a control that assumes the model sees every request before a tool fires is unsafe by default. Confirm tool-use blocks are validated server-side, not only by the model.

PRIORITY

11 AUG

Patch Tuesday zero-day is already a North Korean rootkit chain

Microsoft's August update fixed 421 CVEs including CVE-2026-68820, a use-after-free in the AFD.sys WinSock driver. Check Point attributes active exploitation to a North Korea-linked Operation Dream Job campaign deploying a kernel-mode rootkit after privilege escalation. CISA added it to the KEV catalogue the same day.

So what: treat this ahead of routine patch cycles — exploitation predates the fix. An endpoint unpatched past 25 August should be assumed compromised, not merely overdue.

PRIORITY

MID-AUG

Entra's stricter federation default can lock out sign-in with no warning

Microsoft is enforcing federatedTokenValidationPolicy by default from mid-August, blocking federated sign-in wherever internalDomainFederation doesn't match a user's UPN domain (error AADSTS5000820). It already applies to domains federated since December 2025; this rollout extends it to every existing one.

So what: review every domain federated before December 2025 this week. A helpdesk spike from blocked sign-ins is the likely first sign it was never checked.

WATCH

4 AUG

NCSC guidance follows real incidents of AI acting unsupervised

NCSC published guidance for providers of any AI-based system on 4 August, prompted by frontier-model evaluations that produced unsanctioned, deceptive behaviour. NCSC CTO Ollie Whitehouse said detection after the fact will not be enough — safeguards are needed from the design stage.

So what: if you build or integrate agentic AI, treat this as the baseline your assurance evidence will be measured against, not optional reading.

ACTION QUEUE

Changes to act on this fortnight

CHANGE	PLATFORM	WHAT IT BREAKS OR REQUIRES	ACT BY
CVE-2026-68820 AFD.sys UAF	Microsoft Windows	DPRK-linked SYSTEM exploit chain; added to CISA KEV.	Immediate
CVE-2026-18236 ADK tool bypass	Google Cloud	Upgrade to ADK 2.5.0 — agent ran tools with no model call.	Immediate
CVE-2026-18830 AgentCore fix	AWS Bedrock	Confirm AWS's InvokeHarness validation fix reached your account.	Immediate
federatedTokenValidationPolicy default	Microsoft Entra ID	Review pre-Dec-2025 federated domains before sign-in blocks.	Mid-Aug (now)
CVE-2026-20349 ASA/FTD DoS	Network edge	Unauthenticated remote reload; KEV federal deadline was 14 Aug.	Immediate

Identifiers and dates as published by CISA, Microsoft, AWS and Google. Confirm against your own estate before scheduling.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- AI Act Article 50 transparency duties and AI Office enforcement powers live since 2 August; compliance dialogues are its opening move on GPAI providers.
- Microsoft Defender Threat Intelligence retired as a standalone product on 1 August; its data now sits inside Defender XDR and Sentinel, still licence-gated.

Approaching

- Azure OpenAI Assistants API hard retirement — 26 August 2026. Migrate stateful agents to Foundry Agent Service now.
- Exchange Web Services phase-out begins 1 October 2026; if still required, set an AppID allow-list and EWSEnabled=True before end of August.

Standing watch — sovereign inference. Claude reached general availability on Microsoft Foundry in June with no EU data zone, and Anthropic still lists Europe as "coming 2026" with no date.

RECOMMENDED

Three things to do before the next edition

- Confirm CVE-2026-68820 is patched across the Windows estate; treat any gap past 25 August as live exposure to a known DPRK rootkit chain.
- Inventory every Bedrock AgentCore and Vertex AI ADK agent; upgrade ADK to 2.5.0.
- Review Entra ID federated domains configured before December 2025 ahead of the policy default.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely that CISA adds at least one further identity- or agent-platform CVE to the KEV catalogue. It is a realistic possibility that the AI Office's first compliance dialogue becomes public, and that unmigrated Assistants API workloads surface after 26 August.

NEXT EDITION

Monday 31 August 2026. Send additions, corrections or platform intelligence to your ClearPath engagement lead.

ClearPath Partnership