

Week commencing 12 October 2026

COVERAGE

28 September – 11 October
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...

AWS's own AI-agent platform defaulted to full admin access for anyone, if no identity provider was set.

On 2 October AWS patched Loom, its AI-agent platform: an unconfigured identity provider made the backend return a fixed super-admin identity to any unauthenticated caller (CVSS 10.0). It is September's AEPD pattern again — untrusted access, no human gate — but this time the gap was the vendor's own default. Ask this week: which agent platform still assumes an identity provider nobody configured?

THIS FORTNIGHT

Platform change and AI regulation

PRIORITY

2 OCT

AWS ships emergency fixes across its AI-agent and ML platforms

Two bulletins fixed four flaws. In Loom, an unconfigured identity provider let unauthenticated callers in as super-admin (CVE-2026-103956, CVSS 10.0); two SSRF bugs exposed tokens, fixed in 1.7.0. In SageMaker Unified Studio, a command-injection flaw (CVE-2026-104019, CVSS 9.3) let one project member steal another's credentials.

So what: patch Loom to 1.7.0 and confirm SageMaker Unified Studio runs a supported, patched line — both needed no prior access.

PRIORITY

30 SEP

Entra Connect Sync's hard stop hits hybrid estates still on old builds

Microsoft's back-end hardening change took effect on 30 September: any Entra Connect Sync instance below version 2.5.79.0 stops synchronising entirely. Microsoft calls it a hardening requirement, not a retirement — sync resumes once upgraded — but there is no grace period for the outage itself.

So what: confirm your sync version now — anything below 2.5.79.0 has already stopped, silently breaking directory sync until upgraded.

PRIORITY

4 OCT

Citrix NetScaler flaw hits CISA's KEV; federal deadline already passed

CISA added CVE-2026-88779 to its KEV catalogue on 4 October after Citrix confirmed active exploitation; the federal deadline was 7 October. Confirmed impact is denial of service; remote code execution is still unconfirmed. Fixed in NetScaler 14.1-73.41, 13.1-64.28 and matching FIPS builds — some SAML setups need a second upgrade.

So what: if NetScaler fronts remote access or SSO, patch now and check the SAML build — exploitation followed disclosure within days.

WATCH

1 OCT

Azure retires three AI services; AWS and Google stay quiet this fortnight

Anomaly Detector, Metrics Advisor and Personalizer retired on 1 October, alongside Translator's S2-S4 discount tiers. None had a direct Azure AI Foundry replacement at retirement. AWS and Google Cloud published no comparable platform or pricing changes in this window.

So what: any workload still calling these APIs is already unsupported — assess a replacement now rather than waiting for a failure to force it.

ACTION QUEUE

Changes to act on this fortnight

CHANGE	PLATFORM	WHAT IT BREAKS OR REQUIRES	ACT BY
CVE-2026-103956/7/8 Loom flaws	AWS Loom (AI agents)	Unauthenticated super-admin access via unconfigured identity provider.	Immediate
CVE-2026-104019 SageMaker injection	AWS SageMaker Unified Studio	Cross-tenant code execution, credential theft between project members.	Immediate
Sync enforcement, pre-2.5.79.0	Microsoft Entra Connect Sync	Directory synchronisation stops entirely, no grace period.	Passed — fix now
CVE-2026-88779 NetScaler	Citrix (identity/remote access)	Actively exploited denial of service; RCE still unconfirmed.	Passed — fix now
Anomaly Detector, Metrics Advisor, Personalizer retire	Azure AI	APIs unsupported with no built-in migration path.	Passed — plan now

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

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- AI Act Digital Omnibus (in force since 27 Jul) — Annex III high-risk due 2 December 2027, Annex I 2 August 2028; Article 50 transparency duties remain live throughout.
- Entra Connect Sync’s 30 September enforcement treats hybrid identity hygiene as a hard security gate, not a feature retirement — expect more of this pattern.

Approaching

- Entra Connect Sync 2.5.79.0 reaches end of support 23 October 2026 — plan the next upgrade now, not after this cutover.
- CISA’s remediation windows keep compressing: NetScaler’s ran three days, KEV listing to federal deadline.

Standing watch — sovereign cloud and data residency. No new sovereign-cloud announcements this fortnight; track suppliers’ data-boundary commitments at contract renewal — this moves slower than patching but matters as much.

RECOMMENDED

Three things to do before the next edition

- Patch Loom to 1.7.0 and confirm every instance has an identity provider actually configured.
- Confirm hybrid sync runs Entra Connect Sync 2.5.79.0 or later across every connector in your estate.
- Patch NetScaler to the fixed builds and re-check any SAML-specific upgrade path separately.

OUTLOOK — NEXT FORTNIGHT

Likely: further CVEs surface in AWS’s and Microsoft’s expanding agentic AI tooling as adoption outpaces security review. Realistic possibility: NetScaler’s flaw is reclassified for remote code execution as research continues. Expect no AI Act movement before the AI Office’s delayed guidance lands.

NEXT EDITION

Monday 26 October 2026. See additions, corrections or platform intelligence to your ClearPath or engagement lead.