Week commencing 21 September 2026

ClearPath Partnership

COVERAGE
7–20 September 2026

AUDIENCE
Accountable managers · IT and security leadership

HANDLING
Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING…

The fortnight's biggest UK aviation disruption was a one-millisecond software bug, not an attacker.

A NATS flight-data processing fault on 8 September cancelled over 2,000 flights and stranded roughly 330,000 passengers, worst at Heathrow, Gatwick, Manchester and Birmingham. NATS and the UK's air traffic chief ruled out hostile interference; that took hours to say with confidence. Ask your team: could we tell an accident from an attack that fast, and who is authorised to say so in public.

FORTNIGHT IN REVIEW

Incidents and sector activity

PRIORITY

9–16 SEP

Two maximum-severity Cisco zero-days reach the KEV catalogue within a week

CISA added Cisco Secure Firewall Management Center authentication-bypass flaw CVE-2026-20079 on 9 September — already exploited by nation-state and ransomware actors since August — then Identity Services Engine flaw CVE-2026-76460 on 16 September. Both are CVSS 10.0 and give unauthenticated root access.

So what: FMC sets firewall policy; ISE sets network admission. Confirm both are patched or isolated before anything else this week.

PRIORITY

9 SEP

Citrix NetScaler authentication bypass under active exploitation

Citrix's critical NetScaler ADC/Gateway flaw CVE-2026-19490 (CVSS 9.3) moved from patched to in-the-wild exploitation within days; CISA catalogued it on 9 September, covering AAA and Gateway virtual servers used for SSL VPN, ICA Proxy and RDP Proxy.

So what: NetScaler commonly carries supplier and remote-engineer access. Treat any unpatched internet-facing unit as already compromised.

PRIORITY

9 SEP

Fortinet FortiOS heap overflow added with a forensic-triage requirement

CISA catalogued CVE-2025-25249, a heap-based buffer overflow in FortiOS and FortiSwitchManager (CVSS 9.8), on 9 September, with a 12 September remediation deadline and an unusual instruction: check for prior compromise, not just patch.

So what: if this sits at your network boundary, patch and investigate for existing compromise, not one or the other.

WATCH

7 SEP

Metaencryptor lists aerospace supplier SIFCO Industries

Metaencryptor, previously focused on healthcare, listed Ohio aerospace, energy and defence supplier SIFCO Industries on its leak site on 7 September alongside two other new victims. The claim is unverified beyond the listing; no data sample has been confirmed.

So what: a healthcare-focused group diversifying into aerospace suppliers is an unknown quantity. Check tier-2/3 supplier notification clauses.

PATCH QUEUE

Vulnerabilities to act on this fortnight

IDENTIFIER	PRODUCT	WHY IT MATTERS HERE	ACT BY
CVE-2026-20079	Cisco Secure FMC	Auth bypass to root RCE on the firewall management plane.	Overdue
CVE-2026-76460	Cisco ISE / ISE-PIC	Unauthenticated bypass to root on network admission control.	Overdue
CVE-2026-19490	Citrix NetScaler ADC/Gateway	Auth bypass on VPN, ICA and RDP proxy for remote access.	Overdue
CVE-2025-25249	Fortinet FortiOS / FortiSwitchManager	Unauthenticated RCE at the network boundary. Forensic triage required.	Overdue
CVE-2026-87886	Acronis Cyber Protect/Backup	Incorrect default permissions on back-office and OT backup.	7 days

Identifiers are as published in the CISA KEV catalogue. Confirm applicability against your own asset inventory — this list is a prompt, not a substitute for it.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- Cyber Resilience Act Article 14 reporting began 11 September: manufacturers must file a 24-hour early warning and 72-hour notification for exploited flaws.
- No new EASA Part-IS AMC/GM this fortnight; the 18-month glide path to full PSOE compliance continues.

Approaching

- NIS2: no finalised fine confirmed yet; first enforcement actions are expected before year end.

UK. No new CAA cyber information notice this fortnight; the CAP 1753 oversight cycle continues unchanged.

Standing watch — GNSS interference. Kaliningrad spoofing infrastructure keeps expanding, from a few antennas in 2025 to several dozen; NATO and RAF assets were affected over the Baltic. EASA's Safety Information Bulletin remains operative guidance.

RECOMMENDED

Three things to do before next edition

- Patch or isolate Cisco FMC, ISE and Citrix NetScaler on your estate today; all three are confirmed under active exploitation now.
- Confirm your manufacturers and suppliers can meet the Cyber Resilience Act's 24-hour and 72-hour reporting clocks for exploited flaws.
- Test a same-day runbook for telling a technical outage from a cyberattack, and who is authorised to say which in public.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely a further Cisco or Citrix remote-access product joins the KEV catalogue before the next edition, given three such additions this fortnight. It is a realistic possibility a European ANSP or airport discloses a NATS-style failure that again draws unproven cyberattack claims.

NEXT EDITION

Monday 5 October 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership