Week commencing 16 November 2026

ClearPath Partnership

COVERAGE
2 — 15 November 2026

AUDIENCE
Accountable managers · IT and security leadership

HANDLING
Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING…

A two-year intrusion at a booking-system supplier most passengers have never heard of has just surfaced at a dozen airlines at once.

Amadeus disclosed that a valid admin credential gave an intruder access to reservation data from August 2023 until containment in September 2026. Finnair, Malaysia Airlines, Qantas, Cathay Pacific and others have confirmed exposure. Ask one question: which suppliers hold years, not days, of our passenger data — and would we know if their credentials were already compromised?

FORTNIGHT IN REVIEW

Incidents and sector activity

PRIORITY

10 NOV

Amadeus reservation-platform breach exposes passenger data across a dozen airlines

Amadeus confirmed an intruder used a valid admin credential to reach booking data from August 2023 until containment in September 2026. Finnair (116,000 bookings) and Cathay Pacific (53,000) disclosed figures; Malaysia Airlines, Qantas, Japan Airlines and others confirmed exposure without counts. Contact details and some passport numbers were taken; no payment data, Amadeus says.

So what: one compromised supplier credential touched a dozen carriers at once. Ask whether reservation suppliers monitor and rotate admin credentials, not only customer-facing ones.

PRIORITY

9 NOV

IBM Aspera Faspex file-transfer flaw added to the exploited-vulnerability catalogue

CISA added CVE-2026-123218, a critical (CVSS 9.8) authorisation-bypass flaw in IBM Aspera Faspex 5.0.0–5.0.19, on 9 November, with a three-day federal deadline. A crafted message lets an authenticated user gain full admin privileges. Faspex-class platforms routinely carry MRO and engineering data exchanged with suppliers.

So what: confirm whether any Faspex instance is internet-facing and patch to 5.0.19 PL1 now — the deadline has passed.

PRIORITY

6 NOV

SonicWall SSL VPN SAML bypass confirmed as actively exploited

CISA added CVE-2026-19868 to its catalogue on 6 November. Holding valid credentials for one authentication method lets an attacker bypass SAML-enforced sign-on, including MFA, on SonicOS SSL VPN. SonicWall disclosed six further flaws alongside it; the federal deadline is 20 November.

So what: SonicWall SSL VPN remains common for supplier and engineer access. Check SAML configuration specifically — MFA alone does not block this bypass.

WATCH

ONGOING

Ransomware groups continue targeting aviation and aerospace suppliers

No new named aviation or aerospace victim was confirmed on leak sites this fortnight, but the pattern set by Storm's September listing of wire-harness supplier Star Aviation shows no sign of easing.

So what: no new named victim is not the same as no risk. Keep checking leak-site trackers against your supplier and integrator register, not only your own name.

PATCH QUEUE

Vulnerabilities to act on this fortnight

IDENTIFIER	PRODUCT	WHY IT MATTERS HERE	ACT BY
CVE-2026-123218	IBM Aspera Faspex	File transfer for MRO, engineering and supplier data; crafted message grants full admin.	Overdue
CVE-2026-19868	SonicWall SonicOS SSL VPN	Remote-access route for suppliers and engineers; bypasses SAML-enforced sign-on.	20 Nov
CVE-2026-104935	Ivanti Connect Secure	VPN for supplier and engineer access; zero-day since 1 Oct, deadline passed.	Overdue
CVE-2026-19490	Citrix NetScaler Gateway/AAA	Auth bypass with no workaround; fourth NetScaler addition this year.	Overdue
CVE-2026-20079	Cisco Secure FMC	Management-plane compromise, tied to Sandworm and Qilin activity.	Overdue

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

- EASA Part-IS applies to carriers, MROs, CAMO and ATO since 22 February 2026 — unchanged.
- CRA's 24-hour early-warning duty for exploited vulnerabilities applies to manufacturers since 11 September 2026; no retroactive duty for earlier flaws.

Approaching

- NIS2 baseline measures continue rolling out to member states' aviation entities after Italy's October deadline.
- UK NIS reform legislation continues its passage; CAA CAF cycles unaffected meanwhile.

UK. No new CAA cyber notice this fortnight. The CAA's call for input on September's NATS incident (closing 23 Nov) concerns a software defect, not a cyber attack.

Standing watch — GNSS interference. EASA's Revision 4 bulletin of 3 July, corrected 22 July, remains operative. No new bulletin this fortnight.

RECOMMENDED

Three things to do before the next edition

- Ask which suppliers hold years of booking data via Amadeus or similar platforms, and whether admin credentials are monitored.
- Patch or isolate internet-facing Aspera Faspex and SonicWall SSL VPN instances today; check SAML configuration separately from MFA.
- Cross-check ransomware leak-site trackers against your supplier and integrator register, not just your own name.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely further exploited-vulnerability additions affecting remote-access or file-transfer products follow before the next edition, given five such additions this fortnight alone. It is a realistic possibility a named aviation or aerospace supplier appears on a ransomware leak site before 30 November.

NEXT EDITION

Monday 30 November 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.