Week commencing 2 November 2026

ClearPath Partnership

COVERAGE
19 October – 1 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 VPN used for supplier and engineer access was being exploited as a zero-day weeks before the government's own patch deadline for it passed.

CISA confirmed exploitation of an Ivanti Connect Secure flaw from at least 1 October, but only added it to its exploited-vulnerability catalogue with a 16 October deadline — already overdue by the time this reaches you. Ask one question: for every remote-access product your suppliers and engineers use, how long would exploitation run before anyone noticed.

FORTNIGHT IN REVIEW

Incidents and sector activity

PRIORITY

13 OCT

Ivanti Connect Secure zero-day added to the exploited-vulnerability catalogue

CISA confirmed in-the-wild exploitation of an authentication-bypass flaw (CVE-2026-104935, CVSS 8.6) in Ivanti Connect Secure dating to at least 1 October. The federal remediation deadline of 16 October has already passed. Connect Secure is widely used for VPN access by contractors, engineers and ground-handling suppliers.

So what: treat this as overdue, not merely important. Confirm Connect Secure's version and patch status today, and review who authenticates through it.

PRIORITY

19 OCT

Italy's aviation entities face a new NIS2 baseline security deadline

Italian aviation organisations registered under NIS2 since April 2025 became subject to baseline security measures from October 2026, per legal analysis published 19 October. The obligation sits alongside, not in place of, EASA Part-IS.

So what: if you operate in Italy or rely on Italian suppliers, confirm which baseline measures now apply and when your own transposition deadline falls.

WATCH

27–29 OCT

IATA holds its first dedicated Cybersecurity Summit

IATA's inaugural Cybersecurity Summit convened in Geneva from 27 to 29 October, covering supplier vulnerabilities, offensive AI and divergent national regulatory approaches. No outcomes or communique have been published yet.

So what: a first-of-its-kind summit on supplier risk signals the industry sees third-party exposure, not airline IT itself, as the open problem.

WATCH

ONGOING

Ransomware groups continue to list aviation and aerospace suppliers

No new named victim was confirmed this fortnight, but recent leak-site listings against a US wiring-harness maker and a Brazilian aviation services firm show the supplier-first pattern persisting rather than fading.

So what: check whether any listed victim, or a comparable supplier type, sits in your own or your integrators' supply chain.

PATCH QUEUE

Vulnerabilities to act on this fortnight

IDENTIFIER	PRODUCT	WHY IT MATTERS HERE	ACT BY
CVE-2026-104935	Ivanti Connect Secure	VPN for supplier and engineer remote access; exploited as zero-day since 1 Oct.	Overdue
CVE-2026-0322	Palo Alto PAN-OS	Root RCE on the firewall admin plane; carried over, still unresolved in many estates.	Overdue
CVE-2026-76519	Cisco Secure Email Gateway	Unauthenticated root RCE via an ordinary email attachment.	Overdue
CVE-2026-105133/4	Ahsay AhsayCBS	Chainable auth bypass and command injection in the backup console.	Overdue
CVE-2026-88779	Citrix NetScaler ADC/Gateway	Third distinct NetScaler KEV addition in six weeks.	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

- NIS2 baseline security measures now apply to Italian aviation entities registered since April 2025.
- EASA Part-IS compliance deadline of 22 February 2026 remains unchanged.

Approaching

- Further NIS2 national transposition deadlines continue across member states into 2026–27.
- UK NIS reform legislation continues its passage; CAA CAF assurance cycles unaffected meanwhile.

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

Standing watch — GNSS interference. EASA's Revision 4 bulletin of 3 July, corrected 22 July, remains the operative guidance. No new bulletin this fortnight; Baltic, Black Sea and eastern Mediterranean jamming continues unchanged.

RECOMMENDED

Three things to do before the next edition

- Confirm whether Ivanti Connect Secure runs in your estate and patch it now — the federal deadline has passed.
- Ask your Part-IS or NIS2 lead whether Italy's new baseline deadline changes anything for your suppliers.
- Cross-check this fortnight's named ransomware victims against your supplier and integrator register.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely that at least one further remote-access or identity product joins the KEV catalogue before the next edition, given three Citrix NetScaler additions in six weeks. It is a realistic possibility that IATA publishes outcomes from its Cybersecurity Summit before 16 November.

NEXT EDITION

Monday 16 November 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership