

Week commencing 19 October 2026

COVERAGE

5 – 18 October 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 government's own patch deadline for three exploited products had already passed before this briefing could reach you.

CISA added Palo Alto PAN-OS, Cisco Secure Email Gateway and Ahsay AhsayCBS to its exploited-vulnerability catalogue on 14 October, with a federal remediation deadline of 17 October. Fortnightly cadence is now slower than the exploitation cycle it is meant to track. Ask your team how it closes that gap between editions, not just within one.

FORTNIGHT IN REVIEW

Incidents and sector activity

PRIORITY

14 OCT

Three widely used products added to the exploited-vulnerability catalogue in one day

CISA catalogued Palo Alto PAN-OS management-interface RCE (CVE-2026-0322, three attacker IPs already published), Cisco Secure Email Gateway unauthenticated root RCE (CVE-2026-76519, CVSS 9.8, via a routine email attachment) and Ahsay AhsayCBS backup-software flaws (CVE-2026-105133, CVE-2026-105134) together on 14 October.

So what: confirm exposure today. A firewall management plane, a mail gateway and backup infrastructure were added the same day — the 17 October deadline is already overdue.

WATCH

7–8 OCT

EASA's Part-IS workshop draws over 950 participants

More than 200 attended in person at Cologne and 750 online for EASA's Part-IS Implementation Workshop, covering proportionate implementation, cross-state oversight consistency, and incident and vulnerability management. EASA called the exchange positive; formal materials follow in the coming weeks.

So what: expect authorities to compare what "proportionate" compliance looks like across member states. Benchmark your own maturity before an inspector does it for you.

WATCH

ONGOING

ATNS ransomware-linked OT intrusion remains unresolved three weeks on

South Africa's air navigation provider has published no forensic findings since commissioning an investigation into ransomware-linked malware in weather-service OT. The claimed exfiltration to China-based IP addresses and the possibility of insider involvement both remain open questions.

So what: an unpublished finding is not a closed incident. Keep tracking it as live exposure beside safety-adjacent systems, not a settled story.

WATCH

ONGOING

Qilin's Thai Lion Air claim still unconfirmed

Qilin's 2 October leak-site listing against Thai Lion Air has produced no published data sample and no airline statement. One secondary report links it to a credential-harvesting infostealer said to have taken over 41,000 passwords from the airline; that figure is unverified.

So what: silence on a leak-site listing is not resolution. If a Lion Air group entity sits in your supplier chain, decide your response before data surfaces.

PATCH QUEUE

Vulnerabilities to act on this fortnight

IDENTIFIER	PRODUCT	WHY IT MATTERS HERE	ACT BY
CVE-2026-0322	Palo Alto PAN-OS	Root RCE on the firewall admin plane; three attacker IPs already published.	Overdue
CVE-2026-76519	Cisco Secure Email Gateway	Unauthenticated root RCE via an ordinary email attachment.	Overdue
CVE-2026-105133	Ahsay AhsayCBS	Improper authentication in backup console; weakens your last line of recovery.	Overdue
CVE-2026-105134	Ahsay AhsayCBS	Command injection, chainable with the above for full host compromise.	Overdue
CVE-2026-76504	Cisco Catalyst SD-WAN Manager	Admin auth bypass added 30 Sep; still unresolved in many estates.	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

- CRA Article 14 reporting has applied since 11 September; ground IT and supplier software remain in scope even where avionics are not.
- EASA Part-IS compliance deadline of 22 February 2026 is unchanged; no new AMC/GM beyond the workshop discussion.

Approaching

- Formal Part-IS workshop materials and any resulting guidance are expected within weeks, per EASA.
- IATA Cybersecurity Summit, Geneva, 28–29 October — includes a 2027 aviation threat outlook session.

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 PAN-OS, Cisco Secure Email Gateway or Ahsay AhsayCBS runs in your estate and patch now.
- Ask your Part-IS lead what "proportionate implementation" means for your organisation specifically.
- Track ATNS and the Thai Lion Air claim for confirmed findings before treating either as resolved.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely that at least one further edge or email-security product joins the KEV catalogue before the next edition, given the pace of additions this fortnight. It is a realistic possibility that ATNS or Thai Lion Air publishes confirmed findings before 2 November.

NEXT EDITION

Monday 2 November 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

