

Week commencing 5 October 2026

COVERAGE

21 September — 4 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...

A Citrix NetScaler zero-day sat open to attackers for three weeks before anyone called it a vulnerability.

CVE-2026-88771 and CVE-2026-88772 were exploited from 3 September, planting webshells on NetScaler ADC and Gateway appliances; Citrix disclosed and patched only on 27 September. If NetScaler sits in your estate, assume compromise, not just exposure, and hunt for webshells before trusting the patch. Ask your team when detection on edge appliances was last tested, not just patching.

FORTNIGHT IN REVIEW

Incidents and sector activity

PRIORITY

3–27 SEP

Citrix NetScaler zero-days exploited for three weeks before disclosure

Citrix confirmed CVE-2026-88771 and CVE-2026-88772, both CVSS 9.5, in NetScaler ADC and Gateway on 27 September, after researchers traced exploitation to 3 September. Attackers used the flaws to drop webshells on default configurations, reaching VPN, ICA proxy and RDP proxy services weeks before any patch existed.

So what: patching alone will not remove an existing webshell. Treat any internet-facing NetScaler unit as a forensic question, not just a patch ticket.

PRIORITY

25–30 SEP

Three more products join the exploited-vulnerability catalogue in five days

CISA added SharePoint flaw CVE-2026-65660 and Mikrotik RouterOS flaw CVE-2026-67279 on 25 September, then Cisco Catalyst SD-WAN Manager auth-bypass CVE-2026-76504 (CVSS 9.8) on 30 September — already past its 3 October deadline. Each gives an attacker admin-level control once exposed.

So what: SD-WAN orchestration controls every connected site at once. Confirm Catalyst SD-WAN Manager is patched or isolated today, not scheduled.

WATCH

18–30 SEP

South African ANSP finds ransomware-linked malware in its weather OT network

ATNS, which manages roughly 10% of global airspace, found malware consistent with early-stage ransomware in operational technology supplying weather data for air navigation at Gqeberha, with signs of exfiltration to China-based IP addresses. It has not ruled out insider involvement; no flight disruption has been reported.

So what: weather-feed OT beside safety systems is a realistic target. Confirm your own OT segmentation from general IT — do not assume it.

WATCH

2 OCT

Qilin lists Thai Lion Air on its leak site

Qilin, the group behind this year's Tulsa International Airport and Malaysia Airlines claims, added Thai Lion Air to its leak site on 2 October, threatening to publish data unless negotiations begin. No data sample is yet public and the claim is unverified beyond the listing.

So what: three airline and airport claims from one group this year make the sector a standing target, not a one-off.

PATCH QUEUE

Vulnerabilities to act on this fortnight

IDENTIFIER	PRODUCT	WHY IT MATTERS HERE	ACT BY
CVE-2026-88771	Citrix NetScaler ADC/Gateway	Unauthenticated RCE in default config; exploited weeks before disclosure.	Overdue
CVE-2026-88772	Citrix NetScaler ADC/Gateway	Memory overflow to RCE or denial of service when DTLS is enabled.	Overdue
CVE-2026-76504	Cisco Catalyst SD-WAN Manager	Auth bypass to admin API; controls every connected site at once.	Overdue
CVE-2026-65660	Microsoft SharePoint (on-prem)	Authenticated code injection to remote code execution on internal portals.	7 days
CVE-2026-67279	Mikrotik RouterOS	Unauthenticated session hijack, chainable to full admin access.	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

- CRA Article 14 reporting remains live since 11 September. Aviation-specific products are excluded, but ground IT and supplier software are not automatically.
- No new EASA Part-IS AMC/GM this fortnight; the glide path to full PSOE compliance continues.

Approaching

- EASA Part-IS Implementation Workshop, 7–8 October 2026 — first forum on lessons learned since the February compliance deadline.
- NIS2: four member states have confirmed fines to date, around €765,000 combined; none yet aviation-specific.

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 remains the operative guidance. Jamming and spoofing continue across the Baltic, eastern Mediterranean and Black Sea with no sign of reduction.

RECOMMENDED

Three things to do before next edition

- Hunt for webshells on every NetScaler ADC or Gateway appliance before trusting this month's patch alone.
- Patch or isolate Cisco Catalyst SD-WAN Manager today; its remediation deadline has already passed.
- Confirm OT and weather-feed networks are genuinely segmented from general IT, not just assumed to be.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely a further edge or remote-access product joins the KEV catalogue before the next edition, given five additions this fortnight alone. It is a realistic possibility Qilin or another group names a further airline or airport.

NEXT EDITION

Monday 19 October 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

