Week commencing 24 August 2026

ClearPath Partnership

COVERAGE
10 – 23 August 2026

AUDIENCE
Accountable managers · IT and security leadership

HANDLING
Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING…

Three widely deployed platforms went from patch to mass exploitation in under a week.

VMware vCenter, SharePoint and Windows IKE were each added to the exploited-vulnerability catalogue on 18 August, vCenter alone compromised at 361 organisations within five days of its fix. Ask your team this week: what is our actual time from vendor patch to deployed fix, measured, not assumed.

FORTNIGHT IN REVIEW

Incidents and sector activity

PRIORITY

18 AUG

vCenter, SharePoint and Windows IKE hit by mass exploitation within days of each patch

CISA catalogued four flaws on 18 August: a VMware vCenter Syslog path-traversal (CVE-2026-59310) giving root code execution, exploited at 361 organisations in 47 countries within five days of Broadcom's fix; a SharePoint JWT auth bypass (CVE-2026-55040); and a Windows IKE double-free (CVE-2026-33824), pre-auth over UDP 500/4500.

So what: a monthly patch window no longer protects internet-facing vCenter, SharePoint or IKE VPN endpoints. Treat all three as compromised until patched and checked.

PRIORITY

11 AUG

Cisco ASA and FTD SSL VPN flaw exploited for unauthenticated denial of service

CISA added CVE-2026-20349 after confirming exploitation of a heap-inspection flaw in Cisco ASA and FTD Remote Access SSL VPN. A single crafted, unauthenticated HTTP request forces the device to reload. Federal agencies were ordered to patch by 14 August.

So what: ASA and FTD carry VPN and site-to-site links across airport and airline networks. An unpatched unit can be knocked offline remotely, at will, with no credentials.

WATCH

10 AUG

UAE reports third critical-infrastructure campaign of 2026, aviation among the targets

The UAE Cybersecurity Council said it had detected and contained coordinated intrusion attempts against aviation, energy and education networks, involving phishing and account takeover. No disruption was confirmed. It is the third disclosed sector-wide campaign this year, after finance in July.

So what: Gulf aviation is a live, repeated target. European operators sharing suppliers with Gulf carriers should ask if the same tooling reached them.

WATCH

EARLY AUG

GNSS spoofing over the Baltic now degrades navigation for most transiting aircraft

Lithuania's regulator confirmed Kaliningrad spoofing infrastructure grew from three to 36 transmitters in fifteen months, its radius now reaching Estonia, Latvia, Poland, Finland and Sweden. Over eastern Latvia in early August, roughly three in four aircraft flagged degraded GNSS integrity.

So what: spoofing, not jamming, is now the dominant failure mode. Confirm documented holdover for every ground system with a GNSS timing dependency.

PATCH QUEUE

Vulnerabilities to act on this fortnight

IDENTIFIER	PRODUCT	WHY IT MATTERS HERE	ACT BY
CVE-2026-59310	VMware vCenter	Virtualisation host for much of the estate. Root RCE, exploited within days.	Immediate
CVE-2026-55040	Microsoft SharePoint	JWT auth bypass on internet-facing SharePoint. Full admin impersonation.	Immediate
CVE-2026-33824	Windows IKE (VPN)	Remote-access and site-to-site VPN endpoints. Pre-auth RCE.	Immediate
CVE-2026-20349	Cisco ASA / FTD	Perimeter SSL VPN. Unauthenticated remote crash and reload.	Overdue
CVE-2026-65400	Apple macOS	Auth bypass affecting staff and executive endpoints.	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

- Dutch NIS2 transposition and Critical Entities Resilience Act entered into force 15 August; over 8,000 entities must register with the NCSC.
- The Commission referred Ireland, Spain, France and the Netherlands to the CJEU in early July over incomplete NIS2 transposition.

Approaching

- Cyber Resilience Act manufacturer reporting begins 11 September — 24-hour early warning and 72-hour full notification for actively exploited flaws.

UK. No new CAA cyber information notice this fortnight; the CAP 1753 oversight cycle continues unchanged. No new EASA Part-IS guidance either.

Standing watch — GNSS interference. Kaliningrad spoofing infrastructure keeps expanding; EASA's Safety Information Bulletin revision 4 (3 July) remains the operative guidance as spoofing overtakes jamming as the dominant threat.

RECOMMENDED

Three things to do before next Monday

- Patch or isolate internet-facing vCenter, SharePoint, IKE VPNs and Cisco ASA/FTD today — treat all four as exploited now.
- Confirm GNSS-dependent ground systems and Baltic-transit procedures have documented, tested holdover arrangements.
- Ask Gulf-linked suppliers and partners whether the August UAE campaign used tooling seen against your own estate.

OUTLOOK — NEXT FORTNIGHT

We assess it is highly likely a further internet-facing platform is added to the exploited-vulnerability catalogue within days of its patch release, given three such cases in one week. It is a realistic possibility a European aviation supplier appears on a ransomware leak site before the next edition.

NEXT EDITION

Monday 7 September 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership