Week commencing 3 August 2026

ClearPath Partnership

COVERAGE
27 July – 2 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…

This week's confirmed exploits were not against edge boxes — they were against the consoles that manage them.

CISA confirmed active exploitation of a maximum-severity flaw in Arista's VeloCloud SD-WAN orchestrator and a hardcoded credential in Cisco's firewall management platform, both within three days of each other. Compromise of either gives an attacker the platform that controls every site or device beneath it, not just one appliance. Ask your infrastructure team this week: which of our management planes — SD-WAN, firewall, virtualisation, identity — are reachable from anywhere they should not be, and when were they last checked, not patched.

THIS WEEK

Incidents and sector activity

PRIORITY

27 JUL

Edge and orchestration products added to the exploited-vulnerability catalogue

CISA added Fortinet FortiOS (CVE-2025-68686, an SSL-VPN symlink-persistence patch bypass) and Arista VeloCloud Orchestrator (CVE-2026-16812, unauthenticated OS command injection, CVSS 10.0) to the KEV catalogue. The VeloCloud flaw affects on-premises orchestrators; compromise propagates to every SD-WAN edge they manage.

So what: if any site connects over SD-WAN via an on-premises VeloCloud Orchestrator, patch to 5.2.3.14, 6.1.3.4 or 6.4.2.4 immediately. Check FortiOS for symlink-persistence indicators regardless of prior patch history.

PRIORITY

29 JUL

Hardcoded credential in Cisco Secure Firewall Management Center exploited

Cisco confirmed active exploitation of CVE-2026-20316: a hardcoded low-privileged account in the Secure FMC web interface (CVSS 8.9), chainable with other FMC flaws to escalate privileges. CISA set a federal remediation deadline of 1 August.

So what: FMC manages a firewall estate, not one device. Treat this as an assume-compromise check, not a routine patch — the static account exists until the fixed release is installed.

WATCH

27–30 JUL

Ransomware groups continue naming aerospace and aviation-adjacent suppliers

CRPxO, active only since March 2026, listed ten new US victims on 27 July including MRO Aerospace (military aircraft component overhaul) and Qube Aviation Catering, claiming 87.3GB from the former. Separately, the Kyber group claimed a breach of L3Harris on 30 July; L3Harris had not confirmed it at the time of writing.

So what: CRPxO is newly active and unverified — treat its claims as unconfirmed. Check all three names against your supplier and integrator register regardless; an unconfirmed claim against a real supplier still tells you where to look.

WATCH

29 JUL

VMware vCenter authentication bypass disclosed with no workaround

Broadcom's VMSA-2026-0006 discloses two critical vCenter flaws — CVE-2026-59309 and CVE-2026-59310, both CVSS 9.8 — allowing an unauthenticated attacker to bypass authentication and execute code. No exploitation observed as of publication, and no workaround exists.

So what: vCenter and ESX commonly host virtualised OT and passenger-processing systems. Patch on the vendor's timeline, not the next change window — detection cannot substitute for the update.

PATCH QUEUE

Vulnerabilities to act on this week

IDENTIFIER	PRODUCT	WHY IT MATTERS HERE	ACT BY
CVE-2026-16812	Arista VeloCloud Orchestrator	On-prem SD-WAN orchestration — CVSS 10.0, propagates to every managed edge.	Immediate
CVE-2026-20316	Cisco Secure FMC	Manages the firewall estate. Hardcoded credential, chainable to escalation.	Immediate — deadline passed 1 Aug
CVE-2025-68686	Fortinet FortiOS	SSL-VPN remote access. Patch bypass, exploited.	Immediate
CVE-2026-15409 / -15410 CVE-2026-56155	SonicWall SMA1000 Microsoft AD FS	Contractor and engineer remote access; identity federation. Carried from the 14 July additions.	Confirm patched

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: no new AMC/GM guidance this week. Applicability dates (16 Oct 2025; 22 Feb 2026 for air carriers, Part-145, CAMO and ATO) unchanged.
- NIS2: the Commission referred Ireland, Spain, France and the Netherlands to the CJEU in July over incomplete transposition.

Approaching

- Cyber Resilience Act manufacturer reporting begins 11 September 2026. Aviation-specific products are out of scope — but the edge, identity and virtualisation products in this week's queue are squarely in it.
- Dutch NIS2 transposition (Cyberbeveiligingswet) enters into force 15 August 2026.

UK. No new CAA cyber information notice this week; the CAF for Aviation (CAP 1753) oversight cycle continues unchanged.

Standing watch — GNSS interference. EASA's Revision 4 Safety Information Bulletin (3 July) and the EASA-EUROCONTROL joint action plan continue to describe jamming and spoofing worsening near conflict zones. No change to guidance.

RECOMMENDED

Three things to do before next Monday

- Get written confirmation that FortiOS, VeloCloud Orchestrator and Cisco FMC are patched. "Scheduled" is not an acceptable answer for an internet-facing management plane.
- Check MRO Aerospace, Qube Aviation Catering and L3Harris against your supplier register, including fourth parties.
- Confirm your vCenter/ESX patch plan for VMSA-2026-0006 has a date this week — there is no workaround.

OUTLOOK — NEXT SEVEN DAYS

We assess it is likely that at least one further edge, identity or virtualisation product will be added to the exploited-vulnerability catalogue, given three such additions in the last fortnight. It is a realistic possibility that CRPxO's claims are independently corroborated — treat unconfirmed leak-site claims as a prompt to check exposure, not as confirmed breaches.

NEXT EDITION

Monday 10 August 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership