AVIATION CYBER WEEKLY · EDITION 02

# Week commencing 10 August 2026

ClearPath Partnership

**COVERAGE**
27 July – 9 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…

### Four perimeter and remote-management platforms were added to the exploited-vulnerability catalogue in thirteen days.

FortiOS, Cisco's firewall manager, N-able's remote-monitoring platform and clustered Apache Tomcat all sit at the edge or in the remote-access layer that airports, airlines and their IT suppliers depend on. Ask your team this week: can we confirm patch status and internet exposure for all four, across our own estate and every supplier that touches it, today rather than by next change window?

FORTNIGHT IN REVIEW

## Incidents and sector activity

PRIORITY
1–5 AUG

### N-able N-central remote-monitoring platform exploited to hijack MSP-managed endpoints

N-able confirmed active exploitation of an authentication bypass in its N-central RMM tool from 1 August, bypassing an earlier fix. Attackers used the platform's remote-control function and deployed Cloudflare Tunnel for persistence. CISA added both flaws to its exploited-vulnerability catalogue on 3 and 5 August.

**So what:** any supplier or station using N-central may already be compromised. Confirm build 2026.3.1.7 or later and hunt for unexpected Cloudflare Tunnel activity.

PRIORITY
27 JUL

### FortiOS patch-bypass added to the catalogue — old SSL-VPN compromises can regain persistence

CISA catalogued CVE-2025-68686, a FortiOS flaw letting an attacker who previously breached a device via one of three earlier SSL-VPN CVEs bypass the symlink-removal patch and retain filesystem access. Affects FortiOS 6.4 through 7.6.1.

**So what:** a device patched against the original flaw may still be compromised. Audit any unit with a history of the earlier CVEs for lingering symlinks, not just current patch level.

PRIORITY
29 JUL

### Hardcoded credential in Cisco Secure Firewall Management Center exploited

CISA catalogued CVE-2026-20316, a hardcoded low-privileged account in Cisco Secure FMC's web interface (CVSS 8.9), giving remote unauthenticated access to firewall policy, event logs and configuration data, and chainable to escalate privileges.

**So what:** FMC manages firewall policy across airport and airline networks. Install the fixed release and rotate every exposed credential now.

WATCH
4–5 AUG

### Apache Tomcat encryption-bypass exploited by China-nexus actor, added to the catalogue

CISA catalogued CVE-2026-34486 on 4 August after observing exploitation of clustered Tomcat deployments, including use by a China-nexus group deploying the SNOWLIGHT loader against targets in over 100 countries. Fixes are in 11.0.21, 10.1.54 and 9.0.117.

**So what:** check booking, reporting or back-office applications for clustered Tomcat and patch to the fixed builds this week.

PATCH QUEUE

## Vulnerabilities to act on this fortnight

| IDENTIFIER | PRODUCT | WHY IT MATTERS HERE | ACT BY |
|---|---|---|---|
| **CVE-2026-18577 / -18556** | N-able N-central | MSP monitoring at smaller airports and suppliers. Exploited for persistent remote access. | Immediate |
| **CVE-2025-68686** | Fortinet FortiOS | Perimeter VPN. Bypasses the patch for three earlier exploited flaws. | Immediate |
| **CVE-2026-20316** | Cisco Secure FMC | Manages the firewall estate. Hardcoded credential, chainable to escalation. | Immediate |
| **CVE-2026-34486** | Apache Tomcat (clustered) | Underlies booking and back-office apps. Encryption bypass enables RCE. | By 7 Aug |

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

- No new movement on EASA Part-IS or NIS2 this fortnight. Applicability dates already passed; oversight and audit activity continues unchanged.

### Approaching

- Dutch NIS2 transposition and Critical Entities Resilience Act enter into force 15 August; over 8,000 entities must register with the NCSC.
- Cyber Resilience Act manufacturer reporting begins 11 September — 24-hour early warning for actively exploited flaws.

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

**Standing watch — GNSS interference.** Jamming and spoofing across the Baltic, Black Sea and eastern Mediterranean remain persistent, with spoofing now more prominent than pure jamming. EUROCONTROL estimates up to 38 per cent of European en-route traffic transits affected airspace.

RECOMMENDED

## Three things to do before next Monday

- Patch or isolate FortiOS SSL-VPN, Cisco FMC, N-central and clustered Tomcat now — treat all four as actively exploited today.
- Ask every MSP and IT supplier whether they run N-central and get written confirmation of build 2026.3.1.7 or later.
- Hunt logs for unexpected Cloudflare Tunnel processes and unfamiliar low-privilege FMC web-interface logins.

OUTLOOK — NEXT FORTNIGHT

We assess it is highly likely that further edge or remote-access products are added to the exploited-vulnerability catalogue, given four such additions in the last thirteen days. It is a realistic possibility that a new aviation-linked ransomware claim surfaces before the next edition.

NEXT EDITION

Monday 24 August 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership