Week commencing 17 August 2026

ClearPath Partnership

COVERAGE
3 – 16 August 2026

AUDIENCE
IT and security leadership · compliance and risk leads · programme directors

HANDLING
Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING…

A load balancer and a firewall VPN both joined the federal exploited-vulnerability list this fortnight — both sit at the edge of a typical site estate.

CISA added Progress Kemp LoadMaster (CVE-2026-8037, CVSS 9.6) on 7 August and Cisco Secure ASA/FTD's SSL VPN service (CVE-2026-20349) on 11 August. Both federal deadlines have passed. Ask your infrastructure team this week: which internet-facing appliances are still unpatched against either, and who owns the answer.

THIS FORTNIGHT

Incidents and sector activity

PRIORITY

7–11 AUG

Two more edge products added to the exploited-vulnerability catalogue

CISA added Progress Kemp LoadMaster's command injection flaw (CVE-2026-8037), exploited within days of a public proof of concept, then Cisco ASA/FTD's remote-access SSL VPN flaw (CVE-2026-20349), which crashes the appliance on an unauthenticated request. Both commonly sit in front of contractor remote access.

So what: treat KEV listing as the minimum patch queue regardless of internal CVSS scoring. Confirm both are patched — the 10 and 14 August federal deadlines have passed.

PRIORITY

13 AUG

UK contractor Pacific Construction named on the INC Ransom leak site

INC Ransom listed pacific-construction.com on 13 August, claiming exfiltration of project, client and contract data. Neither the company nor a parent group has issued a public statement; the claim is unverified beyond the leak-site posting.

So what: check the name against your subcontractor register. Confirm your incident response plan covers a leak-site naming, not only encryption.

WATCH

ONGOING, H1 2026

Qilin remains the most active ransomware group worldwide, construction a frequent target

Cyble recorded Qilin as the most active group globally in H1 2026, with 158 attacks across Europe and the UK. It named TIS in April and William Davis Homes in May; INC Ransom's Pacific Construction claim this fortnight extends the same pattern to a second active group.

So what: leak-site naming is now routine for UK construction. Verify fourth-party exposure through every subcontractor and consultant, not only direct suppliers.

WATCH

STANDING RISK

Invoice fraud campaign continues; construction remains disproportionately hit

The NCA and National Federation of Builders' invoice fraud campaign runs through the fortnight, built on figures showing construction and manufacturing together took a quarter of the £3.9m lost to invoice fraud in September 2025 alone — the most recent published NCA data.

So what: make a callback to a previously verified number mandatory for any bank-detail change on a live project, whoever is asking.

ACTION QUEUE

Changes and vulnerabilities to act on this fortnight

CHANGE OR VULNERABILITY	WHAT IT APPLIES TO	WHY IT MATTERS ON A PROJECT	ACT BY
CVE-2026-8037	Progress Kemp LoadMaster	Command injection, CVSS 9.6, exploited at the network edge.	Overdue
CVE-2026-20349	Cisco Secure ASA / FTD	Unauthenticated crash of the remote-access SSL VPN service.	Overdue
Cyber Essentials v3.3	Accounts opened before 27 Apr 2026	MFA and 12-character passwords become automatic-fail controls.	~26 Oct 2026
Gateway 2/3 evidence packs	Higher-risk building projects	Golden thread data must be audit-ready before submission.	Before submission
NCA/NFB invoice fraud guidance	Finance and accounts payable teams	Callback verification stops the sector's costliest cyber loss.	This week

Identifiers as published in the CISA KEV catalogue. Confirm against your own asset inventory.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- Cyber Essentials v3.3 applies to accounts opened since 27 April 2026 — mandatory MFA and a 12-character minimum password.
- BSR Gateway 2 approvals reached 82% nationally (85% remediation, 92% London) to 1 August; median approval time nearly halved to 22 weeks.
- Procurement Act 2023 debarment list remains empty since the regime went live in February 2025.

Approaching

- Cyber Security and Resilience Bill — Lords Committee Stage 1 September 2026. Widens NIS-adjacent duties to supply-chain firms.
- Pre-27 April 2026 Cyber Essentials accounts have until roughly 26 October 2026 to move to v3.3.
- Future Homes Standard confirmed in force from 24 March 2027 (non-higher-risk); plan procurement now.

Standing watch — golden thread evidence gaps. Fragmented metadata and weak document control in CDE platforms still force manual evidence-pack rework ahead of Gateway 2 and 3 submissions. Budget review time before you submit.

RECOMMENDED

Three things to do before the next edition

- Patch or isolate Progress Kemp LoadMaster and Cisco ASA/FTD; both federal deadlines have passed.
- Check Pacific Construction, TIS and William Davis Homes — and their fourth parties — against your register.
- Circulate the NCA/NFB invoice fraud guidance; make callback checks mandatory for bank-detail changes.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely a further edge or remote-access product is added to the exploited-vulnerability catalogue before the next edition, and a realistic possibility another UK construction or engineering firm is named on a leak site, given Qilin's and INC Ransom's current pace.

NEXT EDITION

Monday 31 August 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership