Week commencing 3 August 2026

ClearPath Partnership

COVERAGE
27 July – 2 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…

One hardcoded GitHub credential reportedly gave attackers seven months inside Arup's project data, including HS2 design files.

FulcrumSec's claimed breach of Arup Group traces to a personal access token left in a JavaScript file on a forgotten subdomain — a housekeeping failure, not a sophisticated exploit. The group says it reached over 10,000 repositories, including Oasys and ArupCompute source code and HS2 tunnelling and station design data. Arup has issued no public statement. Ask your design teams this week: where do our access tokens live, and who last audited our public-facing source control.

THIS WEEK

Incidents and sector activity

PRIORITY

27–29 JUL

Three edge and remote-access products added to the exploited-vulnerability catalogue

CISA added Fortinet FortiOS (CVE-2025-68686), Arista VeloCloud Orchestrator (CVE-2026-16812) and Cisco Secure FMC (CVE-2026-20316, hardcoded credentials, remediate by 1 Aug). All three sit in front of the VPN, SD-WAN and firewall estate connecting site cabins, subcontractors and design offices.

So what: treat KEV listing as the minimum patch queue for internet-facing assets, regardless of internal CVSS scoring. Confirm exposure today.

PRIORITY

SINCE 14 JUL, ONGOING

SonicWall SMA1000 zero-days chained by INC ransomware

Two vulnerabilities in the SMA1000 Work Place interface (CVE-2026-15409, CVE-2026-15410), exploited since at least June, let an unauthenticated attacker tunnel into internal services and, when chained, execute code as root. SMA1000 is a common choice for contractor and site remote access.

So what: confirm the vendor patch is applied, not scheduled. INC has already used this pair operationally.

PRIORITY

STANDING RISK

Invoice fraud remains construction's costliest cyber-enabled loss

NCA data show £3.9m lost to invoice fraud in September 2025 alone across 83 cases, with construction and manufacturing together a quarter of reported losses. Attackers compromise a supplier's email thread, then redirect a genuine payment to an account they control.

So what: make a callback to a known, previously verified number mandatory for any bank detail change on a live project — no exceptions.

WATCH

ONGOING

Ransomware groups continue naming UK construction and engineering firms

NCC Group's Q2 data puts construction and engineering among the most-targeted capital-goods sub-sectors, Qilin the most active group globally. William Davis Homes (Qilin, 27 May) and, within this coverage window, digital services provider Caspian One (Deadlock, 26 Jul) were both named.

So what: check both against your supplier and integrator register, including fourth parties reached through subcontractors.

ACTION QUEUE

Changes and vulnerabilities to act on this week

CHANGE OR VULNERABILITY	WHAT IT APPLIES TO	WHY IT MATTERS ON A PROJECT	ACT BY
CVE-2025-68686 / -16812	FortiOS & Arista VeloCloud	Site-to-site and subcontractor remote access. Confirmed exploited.	Immediate
CVE-2026-20316	Cisco Secure FMC	Hardcoded credential, confirmed exploited. CISA deadline 1 Aug.	Immediate
CVE-2026-15409 / -15410	SonicWall SMA1000	Chained SSRF and RCE, used by INC ransomware.	Immediate
Cyber Essentials v3.3	CE / CE+ holders	MFA and a 14-day patch SLA are automatic-fail controls.	Existing accounts by ~27 Oct

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

- Procurement Act 2023 debarment regime, live since Feb 2025. Investigations into seven Grenfell-linked firms remain paused at the request of the CPS and Met Police.
- Cyber Essentials v3.3 applies to accounts opened since 27 April 2026 — mandatory MFA, 14-day critical-patch SLA.
- CDM 2015 unchanged — HSE's five-year review confirms it remains fit for purpose.

Approaching

- Cyber Security and Resilience Bill — Lords Committee 1 September 2026, Royal Assent expected late 2026. Widens NIS-adjacent duties to more supply-chain firms.
- Existing Cyber Essentials accounts have until roughly 27 October 2026 to move to v3.3.
- Gateway 3 evidence packs must be audit-ready before occupation; BSR guidance stays thin.

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

RECOMMENDED

Three things to do before next Monday

- Patch or isolate FortiOS, VeloCloud Orchestrator, Cisco FMC and SonicWall SMA1000 across the internet-facing estate.
- Sweep public repositories and subdomains for hardcoded credentials; the Arup breach reportedly began with one.
- Circulate the NCA/NFB invoice fraud advisory and make a callback to a known number mandatory for any bank detail change.

OUTLOOK — NEXT SEVEN DAYS

We assess it is likely that a further remote-access or identity product is added to the exploited-vulnerability catalogue this week, and a realistic possibility that another UK construction or engineering firm is named on a ransomware leak site, given Qilin's and Deadlock's current focus. Both test whether your patch and credential hygiene move faster than the attackers.

NEXT EDITION

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

ClearPath Partnership