Week commencing 31 August 2026

ClearPath Partnership

COVERAGE
17 – 30 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 forged-token bypass in on-premises SharePoint reached the federal exploited list this fortnight — many contractors run their document platform on it.

CISA added CVE-2026-55040 on 18 August: an unauthenticated attacker can forge a valid token against on-premises SharePoint, bypassing login entirely. SharePoint remains a common project extranet and document platform. Ask this week: is ours patched, and if it faces the internet, why?

THIS FORTNIGHT

Incidents and sector activity

PRIORITY

18 AUG

SharePoint and vCenter join the exploited-vulnerability catalogue together

CISA added Microsoft SharePoint's authentication bypass (CVE-2026-55040) and Broadcom VMware vCenter's path traversal flaw (CVE-2026-59310) on 18 August, both CVSS 9.8, alongside Windows IKE and macOS flaws. SharePoint commonly hosts project extranets; vCenter underpins servers many contractors run on.

So what: confirm patch status on any internet-facing SharePoint or vCenter instance today. Federal remediation was due 21 August — treat that as your own deadline.

PRIORITY

30 AUG

UK consultancy named on Qilin's leak site

Qilin claimed Absolute Consultancy Services, a UK-based firm, on 30 August, listing disruption to company systems and data. Neither the company nor a client has issued a public statement; the claim is unverified beyond the leak-site posting.

So what: check the name against your consultant and subcontractor register, including any design or advisory work reaching live projects.

WATCH

Q1 2026 DATA

Construction climbs to the fourth most-targeted sector for ransomware

GuidePoint's GRIT report recorded 131 construction ransomware victims in Q1 2026, up 44% year-on-year, moving the sector from sixth to fourth most affected globally, behind only manufacturing, technology and healthcare.

So what: budget on the assumption attackers now see construction as a soft, high-value target, not a niche one.

WATCH

STANDING RISK

Payment diversion fraud remains construction's costliest cyber loss

UK construction firms lost over £200,000 in Q1 2026 to payment diversion scams, where criminals impersonating suppliers or colleagues redirect bank-detail changes on live projects — still more costly in aggregate than encryption events.

So what: make a callback to a previously verified number mandatory for any bank-detail change, 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-2026-55040	Microsoft SharePoint (on-prem)	Forged token bypasses login on project extranets and CDEs.	Overdue
CVE-2026-59310	Broadcom VMware vCenter	Path traversal on the platform hosting many project servers.	Overdue
Cyber Security and Resilience Bill	CNI-adjacent and supply-chain firms	Committee Stage; widens duties to designated "critical suppliers".	1 Sept 2026
Building Safety Levy	New-dwelling and student housing schemes	New payment condition attached to building control approval.	1 Oct 2026
Payment diversion fraud	Finance and accounts payable teams	Sector's costliest cyber loss; callback verification stops it.	Standing

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

- BSR Gateway 3 approvals reached 72% on 29 determinations to 1 August; median time 16 weeks, the quickest in eight weeks.
- Gateway 2 approvals held at 82% nationally over the same 12-week period, per BSR transparency data.
- Procurement Act 2023 debarment list remains empty since the regime went live in February 2025.

Approaching

- Cyber Security and Resilience Bill reaches Lords Committee Stage 1 September 2026, widening duties to "critical suppliers".
- Building Safety Levy takes effect 1 October 2026 for new-dwelling and student housing schemes.
- Pre-27 April 2026 Cyber Essentials accounts have until roughly 26 October 2026 to move to v3.3.

Standing watch — Cyber Essentials Plus flow-down. More Tier-1 frameworks now specify Plus, not standard Cyber Essentials, in PQQ and SSIP packs. Check which live bids require the higher standard before renewal.

RECOMMENDED

Three things to do before the next edition

- Patch or isolate internet-facing SharePoint and vCenter; federal deadlines passed 21 August.
- Check Absolute Consultancy Services and its clients against your subcontractor register.
- Confirm which live bids or frameworks now require Cyber Essentials Plus, not standard CE.

OUTLOOK — NEXT FORTNIGHT

We assess it is highly likely a further edge or identity product joins the exploited-vulnerability catalogue before the next edition, and a realistic possibility another UK construction or consultancy firm is named on a leak site, given Qilin's pace and the sector's rising ransomware share.

NEXT EDITION

Monday 14 September 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership