Week commencing 28 September 2026

ClearPath Partnership

COVERAGE
14 – 27 September 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…

The tools that manage your identity and remote access are this fortnight's biggest exposure, not the systems they protect.

Cisco confirmed a maximum-severity, unauthenticated bypass in Identity Services Engine this fortnight, and two remote-monitoring platforms MSPs use to reach client sites — ConnectWise ScreenConnect and N-able N-central — remain under active exploitation. All three grant root-level control of whatever they manage. Ask this week: which of these three sit in our estate or our MSP's, and are they patched.

THIS FORTNIGHT

Incidents and sector activity

PRIORITY

16 SEP

Maximum-severity Cisco identity platform flaw exploited

CISA added CVE-2026-76460 to its exploited-vulnerability catalogue on 16 September: an unauthenticated API bypass in Cisco Identity Services Engine, CVSS 10. Exploitation grants root-level admin access, letting an attacker rewrite authentication and network-access policy for every device the platform controls.

So what: confirm today whether any ISE deployment is internet-facing or otherwise reachable, and patch immediately. Treat any unpatched instance as already compromised.

PRIORITY

EARLY SEP, ONGOING

Two MSP remote-management platforms under mass exploitation

ConnectWise ScreenConnect (CVE-2026-84869) and N-able N-central (CVE-2026-86218), both patched in early September, remain under confirmed active exploitation — giving unauthorised file execution or full remote code execution on client systems reached through the console.

So what: ask whoever manages your site IT which platform they run and whether it is patched. One compromised console can reach every connected site at once.

WATCH

H1 2026, ONGOING

Qilin remains the most active operator against UK targets

Qilin's leak site listed up to 37 UK organisations through H1 2026, more than any other group, with construction among its most-hit sectors. No new UK construction victim was confirmed this fortnight, but the group's pace against the sector has not slowed.

So what: check new leak-site postings against your supplier and subcontractor register every week, not only when a name looks familiar.

WATCH

ONGOING

Payment diversion fraud continues to outpace encryption losses

The National Crime Agency and National Federation of Builders' joint campaign highlights payment diversion fraud costing the sector over £200,000 in Q1 2026 alone, with deepfake and business-email-compromise tactics growing more convincing across long subcontractor payment chains.

So what: require a callback to a known number before changing any bank detail, whatever the email or call sounds like.

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-2026-76460	Cisco Identity Services Engine	Root-level bypass of the platform controlling network identity and access.	Overdue
CVE-2026-84869	ConnectWise ScreenConnect	Unauthorised file execution via an active remote-management session.	Immediate
CVE-2026-86218	N-able N-central	Pre-auth remote code execution on the console your MSP may use.	Immediate
Second staircase mandate	New residential buildings 18m and over	New design requirement for applications from this date.	30 Sep 2026
Building Safety Levy	New-build and student schemes over 10 units	New payment condition on building control applications.	1 Oct 2026

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

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- Cyber Security and Resilience Bill reached Report Stage in the Lords in September, widening NIS duties to MSPs, data centres and critical suppliers.
- Cyber Essentials v3.3 applies to all assessment accounts created since 27 April 2026: MFA is now pass/fail and cloud services cannot be scoped out.

Approaching

- Second staircase mandate takes effect 30 September for new residential buildings 18 metres and over.
- Building Safety Levy takes effect 1 October for new-dwelling and student schemes over 10 units.
- Pre-27 April 2026 Cyber Essentials accounts must migrate to v3.3 by around 26 October.

Standing watch — golden thread data custody. No BSR enforcement action yet turns on failing to hand over digital building information, but the duty is live for every occupied higher-risk building. Confirm who owns access to yours.

RECOMMENDED

Three things to do before the next edition

- Confirm whether Cisco ISE, ScreenConnect or N-central sit in your estate or your MSP's, and patch now.
- Check this fortnight's leak-site postings against your supplier and subcontractor register.
- Confirm payment-detail changes require a callback to a known number, not just an email reply.

OUTLOOK — NEXT FORTNIGHT

We assess it is highly likely a further identity or remote-management platform joins the exploited-vulnerability catalogue before the next edition, and a realistic possibility a UK construction supplier is named on a leak site, given Qilin and Akira's continued pace against the sector.

NEXT EDITION

Monday 12 October 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership