

# Week commencing 26 October 2026

## COVERAGE

12 – 25 October  
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 root-level firewall flaw with no workaround has landed on the same perimeter products that front your site networks.

CISA added four actively exploited flaws to its KEV catalogue this fortnight, including a PAN-OS management-interface flaw Palo Alto says has no workaround. The affected products front remote access and backup across distributed site estates. Ask this week: which PAN-OS, Cisco Secure Email Gateway or Ahsay AhsayCBS instances do we run, and are they patched.

## THIS FORTNIGHT

### Incidents and sector activity

#### PRIORITY

14 OCT

#### CISA adds four actively exploited flaws in perimeter and backup products

The KEV catalogue gained a PAN-OS management-interface flaw (CVE-2026-0322) giving root code execution with no workaround, a critical Cisco Secure Email Gateway path-traversal bug (CVE-2026-76519) Cisco confirms is under attack, and two Ahsay AhsayCBS backup-software flaws, one a command injection. The federal remediation deadline fell on 17 October.

**So what:** check whether any PAN-OS, Secure Email Gateway or AhsayCBS instance sits in your estate, and patch or isolate now — the remediation window has passed.

#### WATCH

26 OCT

#### Vendor-direction power reaches the Lords floor as the Bill nears a decision

The Cyber Security and Resilience Bill reaches report stage today, with the vendor-direction amendment flagged in our last edition — letting regulators direct how critical suppliers respond to threats — still live for debate. No result was available as this briefing closed.

**So what:** if you supply CNl operators, check the outcome this week — the power could reach your contract terms directly.

#### WATCH

27 OCT

#### Cyber Essentials transition window closes with no grace period

The six-month transition following April's Cyber Essentials v3.3 update ends tomorrow. Assessment accounts opened before the cutover lose the option to certify against the outgoing question set from that date.

**So what:** confirm your account's creation date and submit now if you are still on the old question set — tenders citing Cyber Essentials as a prerequisite will not wait.

#### WATCH

ONGOING

#### No new UK construction victim named this fortnight — fraud remains the costlier pattern

No fresh leak-site naming of a UK construction firm was confirmed in this window. The NCA's construction payment-diversion campaign still cites average quarterly losses near £210,000 to invoice fraud — a steadier drain than any single ransomware event.

**So what:** do not read a quiet fortnight as reduced risk. Check payment-approval controls against diversion fraud, not just the ransomware patch queue.

## 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      |
|------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------|-------------|
| <b>CVE-2026-0322</b>               | Palo Alto PAN-OS mgmt interface    | Root-level RCE, no workaround; common firewall at site and VPN edges.                      | Overdue     |
| <b>CVE-2026-76519</b>              | Cisco Secure Email Gateway         | Critical path traversal; Cisco confirms active exploitation.                               | Overdue     |
| <b>CVE-2026-105133/4</b>           | Ahsay AhsayCBS backup              | Auth bypass and command injection in backup software protecting document and BIM archives. | Overdue     |
| Cyber Essentials transition closes | Pre-April v3.3 assessment accounts | Last window to certify under the outgoing question set.                                    | 27 Oct 2026 |
| CS&R Bill report stage             | CNI suppliers, MSPs, data centres  | Vendor-direction amendment reaches a floor decision.                                       | 26 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

- Building Safety Levy and the second staircase mandate remain live, each with its transitional exemption for schemes already in the system.
- Cyber Essentials v3.3's MFA pass/fail rule applies to every assessment account opened since 27 April 2026.

## Approaching

- Cyber Essentials Plus candidates have until 27 January 2027 to recertify under the old question set once Cyber Essentials itself has closed.
- CS&R Bill report stage lands today; watch for the vendor-direction power's final shape.

**Standing watch — payment diversion fraud.** No new figures this fortnight, but the pattern behind the NCA's campaign has not eased. Treat invoice and bank-detail changes on live projects as a standing control, not a one-off check.

## RECOMMENDED

## Three things to do before the next edition

- Confirm no PAN-OS management interface is reachable beyond trusted IPs, and patch to a fixed release.
- Check Cisco Secure Email Gateway and Ahsay AhsayCBS versions against the fixed builds immediately.
- Submit or renew Cyber Essentials now if your account predates the 27 April 2026 question-set change.

## OUTLOOK — NEXT FORTNIGHT

We assess it is likely further KEV additions reach products common to site estates before the next edition, and a realistic possibility report stage narrows or extends the vendor-direction power materially. There is also a realistic possibility a UK construction victim is named on a leak site, given the sector's continued targeting.

## NEXT EDITION

Monday 9 November 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

