Week commencing 9 November 2026

ClearPath Partnership

COVERAGE
26 October – 8 November 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…

Three different perimeter products gained actively exploited flaws within the same ten days.

GitLab self-managed, Cisco's ASA/FTD firewalls and Ivanti Connect Secure — all common at the VPN and remote-access edge of distributed site estates — each joined CISA's exploited-vulnerability catalogue between 29 and 30 October. Ask this week: which of these three sit in our estate, and are they patched.

THIS FORTNIGHT

Incidents and sector activity

PRIORITY

29-30 OCT

CISA adds GitLab, Cisco and Ivanti flaws to its exploited-vulnerability catalogue

GitLab Community and Enterprise Edition (self-managed) gained CVE-2026-97229, a maximum-severity unauthenticated RCE fixed in 19.2.8/19.3.5/19.4.2. Cisco Secure Firewall ASA/FTD gained CVE-2026-76418, an exploited flaw that forces a device reload. Ivanti Connect Secure gained two more flaws (CVE-2026-111357, CVE-2026-118527) chained with the auth-bypass Ivanti disclosed on 13 October.

So what: patch or isolate any GitLab self-managed instance, Cisco ASA/FTD device or Ivanti Connect Secure appliance now — the federal remediation deadlines have already passed.

WATCH

26 OCT-2 NOV

Lords defeat government twice on the Cyber Security and Resilience Bill

Report stage closed on 26 October with two government defeats: Lord Birt's amendment on the bill's future scope passed 202 to 155, and a second amendment on annual review of covered organisations also passed. Third Reading was listed for 2 November, after which the bill returns to the Commons; no confirmed result of that sitting was available as this briefing closed.

So what: if you supply CNI operators or MSPs, track the Commons stage — the vendor-direction and scope provisions are not yet settled.

WATCH

27 OCT

Cyber Essentials Willow question set closes as scheduled

The transition flagged in our last edition closed on 27 October. New assessments now use only the Danzell (v3.3) question set. Cyber Essentials Plus candidates who began under Willow have until 27 January 2027 to complete.

So what: confirm any assessment started before 27 April is finished, or restarted under Danzell, well ahead of the January deadline.

WATCH

ONGOING

Robert Hitchins Limited leak claim remains unconfirmed

The majinahanashi group's 12 October claim against the Gloucestershire developer, with publication threatened for 15 October, has not been confirmed by the company or a second source nearly four weeks on. Treat leak-site claims as a prompt to check exposure, not as confirmed fact.

So what: if you work with Robert Hitchins on live projects, ask directly rather than waiting for a leak that may never surface.

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-2026-97229	GitLab CE/EE, self-managed	Max-severity unauthenticated RCE on self-hosted delivery-team tools.	Overdue
CVE-2026-76418	Cisco Secure Firewall ASA/FTD	Exploited DoS reload on VPN devices fronting site networks.	Overdue
CVE-2026-111357/118527	Ivanti Connect Secure	Privilege escalation and file upload, chained with 13 Oct bypass.	Overdue
Cyber Essentials Danzell question set	All new CE/CE Plus assessments	Willow closed; Plus candidates under Willow must finish.	27 Jan 2027
CS&R Bill Commons consideration	CNI suppliers, MSPs, data centres	Lords-amended scope and vendor-direction return to MPs.	Watch Nov

Identifiers as published in the CISA KEV catalogue and IASME scheme guidance. Confirm against your own asset inventory before acting.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- Cyber Essentials Danzell (v3.3) is now the only question set for new assessments, since the Willow transition closed on 27 October.
- CISA's KEV catalogue gained three more actively exploited perimeter products this fortnight.

Approaching

- Cyber Essentials Plus candidates assessed under Willow have until 27 January 2027 to complete under the outgoing question set.
- The CS&R Bill returns to the Commons after Lords Third Reading, with scope and vendor-direction provisions still unsettled.

Standing watch — payment diversion fraud. No new figures this fortnight. The NCA's construction campaign still cites average quarterly losses near £210,000 — a steadier drain than any single ransomware event. Keep invoice and bank-detail checks as a standing control.

RECOMMENDED

Three things to do before the next edition

- Patch or isolate any GitLab self-managed instance, Cisco ASA/FTD device or Ivanti Connect Secure appliance now.
- Check which Cyber Essentials or Plus assessments still sit on Willow and plan completion before January.
- Track the CS&R Bill's Commons stage before briefing the board on vendor-direction exposure.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely further KEV additions reach perimeter or remote-access products before the next edition, given three in this fortnight alone. It is a realistic possibility the Commons amends the Lords' scope changes before 23 November, and a realistic possibility the Robert Hitchins claim is confirmed or withdrawn within the fortnight.

NEXT EDITION

Monday 23 November 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership