

Week commencing 12 October 2026

COVERAGE

28 September – 11 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...

The gateway device at the edge of your site network is this fortnight's most urgent patch — and CISA's deadline to fix it has already passed.

Citrix confirmed active exploitation of NetScaler ADC and Gateway, used widely for site and supplier remote access, before a patch existed. CISA's federal deadline fell on 7 October, five days before this briefing. Ask this week: does any appliance in our estate or a subcontractor's run NetScaler with SAML, and is it on a fixed build?

THIS FORTNIGHT

Incidents and sector activity

PRIORITY

4 OCT

Actively exploited NetScaler flaw added to CISA's catalogue

CISA added CVE-2026-88779, a Citrix NetScaler memory-overflow flaw, to its exploited-vulnerability catalogue after confirmed in-the-wild attacks crashed appliances. Exploitation targets SAML configurations; Citrix says it has found no data-integrity impact so far.

So what: confirm whether any NetScaler using SAML sits in your estate, and patch to the fixed builds now — the federal deadline has already passed.

PRIORITY

30 SEP – 1
OCT

Two building-safety deadlines land in the same week

The second staircase mandate for residential buildings 18 metres and over took effect 30 September, and the Building Safety Levy followed on 1 October after a year's delay, applying to new-build and student schemes of ten or more units.

So what: confirm which live schemes fall under each transitional exemption, and whether levy-exempt applications were filed before the cut-off.

WATCH

29 SEP

Extortion group claims a UK facade contractor, as sector risk data hardens

New extortion group NOn listed UK facade engineer Precision Facades Ltd on its leak site, claiming tender data and board papers; the firm has not confirmed this and one tracker questions the sector fit. Cyble separately rated the UK Europe's most ransomware-hit country in Q1 2026, with construction fourth most impacted worldwide, up 44 per cent year on year.

So what: treat an unverified leak-site claim as a prompt to check your own register, not as confirmation — the sector trend behind it is not in doubt.

WATCH

7 SEP,
ONGOING

NIS-reform bill nears report stage with a new supplier power in play

The Cyber Security and Resilience Bill completed Lords committee stage with a vendor-direction-power amendment left untabled for debate. Report stage is set for 26 October, just after this briefing's window — the power would let regulators direct how critical suppliers respond to threats.

So what: if you supply CNI operators, read the amendment before report stage — it could reach your contract terms directly.

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-2026-88779	Citrix NetScaler ADC/Gateway (SAML)	Common remote-access gateway for site and supplier links; confirmed exploited.	Overdue
Cyber Essentials Willow cut-off	Pre-v3.3 assessment accounts	Last window to submit under the outgoing question set.	27 Oct 2026
CS&R Bill report stage	CNI suppliers, MSPs, data centres	Vendor-direction amendment returns to the Lords floor.	26 Oct 2026
Building Safety Levy	New-build/PBSA schemes, 10+ units	Now live; applications before 1 Oct remain exempt.	In effect
Second staircase mandate	Residential buildings 18m and over	Relief needs foundations poured within 18 months.	30 Mar 2028

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

- Second staircase mandate and Building Safety Levy are both live, each with a 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

- Willow-version Cyber Essentials submissions close 27 October 2026; Cyber Essentials Plus candidates have until 27 January 2027.
- Cyber Security and Resilience Bill reaches Lords report stage 26 October, with the vendor-direction power in play.

Standing watch — golden thread data custody. No enforcement action has yet turned 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 any NetScaler appliance in your estate or a subcontractor's uses SAML, and patch now.
- Check your Cyber Essentials account's creation date, and plan your submission before 27 October.
- If you supply CNI operators, read the vendor-direction amendments before report stage on 26 October.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely further edge-gateway exploitation is confirmed before the next edition, and a realistic possibility report-stage debate narrows or extends the vendor-direction power materially. There is also a realistic possibility this fortnight's leak-site claim resurfaces with fresh detail.

NEXT EDITION

Monday 26 October 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

