Week commencing 14 September 2026

ClearPath Partnership

COVERAGE
31 August – 13 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…

A maximum-severity firewall flaw is being exploited by a Russian state actor and a ransomware gang at the same time.

Cisco confirmed CVE-2026-20079, a CVSS 10 authentication bypass in Secure Firewall Management Center, is being exploited by both a Sandworm-linked implant and Qilin ransomware affiliates. FMC controls firewalls across multi-site estates. Ask this week: is ours internet-facing, patched, and would we notice unauthorised admin access before an attacker did.

THIS FORTNIGHT

Incidents and sector activity

PRIORITY

9 SEP

Cisco firewall management plane exploited by state and ransomware actors

CISA added CVE-2026-20079 to its exploited catalogue on 9 September. A Sandworm-linked implant and, separately, Qilin ransomware affiliates are both using it to gain root access to FMC, which manages firewalls across distributed contractor estates.

So what: patch or isolate any internet-facing FMC today. The CVSS 10 score means root compromise, and two distinct threat types are already exploiting it.

PRIORITY

1–9 SEP

Two more VPN gateways join the exploited-vulnerability catalogue

SonicWall's chained SMA1000 zero-days (CVE-2026-83548, -83549) give unauthenticated RCE, disclosed 1 September; Citrix's NetScaler bypass (CVE-2026-19490) has been mass-exploited since 3 September. Both are remote-access gateways used for site and supplier connections.

So what: both sit at the network edge in front of remote access. Confirm patch status today — treat any unpatched internet-facing instance as compromised.

PRIORITY

13 SEP

UK scaffolding contractor named on Qilin's leak site

Qilin listed Gilco Scaffolding, a UK contractor, on its leak site on 13 September, claiming disruption to files and systems. Neither party has commented; the claim is unverified beyond the posting. Qilin is also behind this fortnight's Cisco FMC ransomware intrusions.

So what: check the name against your scaffolding, temporary works and plant-hire suppliers, and confirm Qilin has no foothold elsewhere in your chain.

WATCH

3 SEP

Site routers exposed as MikroTik exploit chain gives full control

A chain dubbed MikroTrick lets an unauthenticated attacker fully compromise internet-reachable MikroTik RouterOS devices via SSH, combining CVE-2026-67277 with privilege escalation CVE-2026-86060. MikroTik patched both on 3 September; over 122,000 devices remain exposed worldwide.

So what: site cabins and compounds often run consumer-grade routers with SSH left open. Check yours are patched and not internet-reachable.

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-2026-20079	Cisco Secure FMC	Root-level compromise, exploited by state and ransomware actors alike.	Overdue
CVE-2026-83548/9	SonicWall SMA1000	Chained flaws give unauthenticated RCE on VPN gateways.	Immediate
CVE-2026-19490	Citrix NetScaler ADC/Gateway	Mass-exploited auth bypass on SSL VPN and remote-access paths.	Immediate
Cyber Security and Resilience Bill	CNI-adjacent and critical suppliers	Lords Committee Stage under way; widens NIS duties and powers.	Monitor
Building Safety Levy	New-build schemes over 10 dwellings	New payment condition before completion certificates issue.	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

- Gateway 2 requirements dispensed with from 1 September for fibre cabling and rooftop mast work; competence and golden thread duties still apply.
- Cyber Security and Resilience Bill entered Lords Committee Stage 1 September, widening NIS duties to "critical suppliers" and data centres.
- Procurement Act 2023 debarment list remains empty 19 months in.

Approaching

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

- Patch or isolate internet-facing Cisco FMC, SonicWall SMA1000 and Citrix NetScaler — all three face active exploitation.
- Check Gilco Scaffolding against your scaffolding, temporary works and plant-hire supplier register.
- Confirm site routers are not internet-reachable via SSH and run patched MikroTik firmware.

OUTLOOK — NEXT FORTNIGHT

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

NEXT EDITION

Monday 28 September 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership