PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

IoT Exploitation Arsenal Expands. Perimeter Defenses Mapped.

A 22-CVE botnet recruitment platform, a coordinated scanner fleet mapping enterprise perimeter defenses, and vulnerability chaining in the React/Next.js campaign mark a week defined by specialization across the exploitation supply chain.

188.0M	22	4x	14
TOTAL SESSIONS OBSERVED	CVES IN IOT EXPLOIT ARSENAL	MID-WEEK SESSION SURGE	WEEKS OF REACT CAMPAIGN

WHAT'S INSIDE

1 VPSVAULT IoT Platform Deploys 22-CVE Arsenal

Four source IPs from AS215925 collectively exploit 22+ vulnerabilities targeting Hikvision cameras, MikroTik routers, TP-Link devices, D-Link NAS, and consumer DVRs. Combined 3,347,443 sessions in a systematic botnet recruitment operation including Generic IoT Default Password Attempt activity.

2 VisionHeight Fleet Maps Enterprise Perimeters

Six AWS-hosted IPs sharing identical fingerprints and rDNS (scan.visionheight[.]com) mapped management interfaces across Palo Alto, Sophos, Ivanti, Citrix, F5, and ConnectWise platforms. 5,892,055 combined sessions checking for authentication bypass vulnerabilities including Palo Alto Networks Login Scanner.

3 React/Next.js Vulnerability Chaining Emerges

CVE-2025-55182 (CVSS 10.0) now chained with Next.js CVE-2025-29927 (CVSS 9.1), defeating both authentication and application security layers in a single operation. 1,338,336 sessions in week 14 via React Server Components CVE-2025-55182 RCE Attempt.

4 Mid-Week Surge Reveals Multi-Operator Activation

Daily sessions quadrupled from 8.5M to 36.6M between Tuesday and Thursday as at least four independent scanning operations — including ICS/SCADA protocol reconnaissance — activated new infrastructure simultaneously.

Want the full brief?

GreyNoise customers get complete IOCs, infrastructure attribution, and role-based recommendations every week.

greynoise.io/contact