PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Exploitation Arrived in Same-Day Cohorts

Adversaries targeted several unrelated flaws on the same day, each at roughly the same source count. Some cohorts ended within that day while others kept running. Adversaries escalated a Next.js authorization bypass across the final three days, and source sets of matched size appeared on eight of nine legacy Citrix flaws in a single day. The single-day cohorts are the harder problem: they never sustain enough volume to cross a rate threshold. Counting distinct sources per product family per day is what catches it.

495
NEXT.JS BYPASS DAILY SOURCES ON A PARTIAL FINAL DAY, FROM NO MORE THAN 3 EARLIER

8 of 9
LEGACY CITRIX FLAWS WITH SOURCE SETS OF MATCHED SIZE, ONE DAY

~1 in 10
OF OBSERVED TRAFFIC, FROM ONE LINKED GROUP OF HOSTS

99.5%
NEXT.JS BYPASS SOURCES CLASSIFIED MALICIOUS, 798 OF 802

WHAT'S INSIDE

1 A Next.js authorization bypass escalated over three days

CVE-2025-29927 lets a caller add one HTTP header so the framework skips its middleware, where many applications place their authentication checks. The application then logs the request as authorized. It is rated CVSS 9.1 and absent from CISA KEV. Daily unique sources went from no more than three to 28, then 426, then 495 across a partial final day. The population was still rising when the window closed.

2 Adversaries checked for eight of nine legacy Citrix flaws in a single day

On 30 August, source sets of matched size appeared on eight of nine Citrix flaws. The products are SD-WAN appliances, XenMobile Server and ShareFile StorageZones, and the ninth, a directory traversal check, stayed at three. All nine produced fewer than 1,000 attempts between them across eight days, so each ranks as minor alone. One of the nine, CVE-2019-12989, is rated CVSS 9.8 and is KEV-listed; the two 2020 flaws are rated 7.5; the remaining six carry no CVSS score, which is itself why a severity-ordered queue never surfaces them. Work all nine as a single inventory pass.

3 A self-declared scanning user agent linked a sweep across four networks

Rented hosts on four networks, 96 in total, ran one scanning toolkit. A self-declared scanning user agent that appears almost nowhere else is confirmed on 43 of them, and the same client fingerprint on 38, though a fingerprint alone marks a tool class rather than an operator. Together they produced roughly a tenth of all traffic observed. A control scoped to any single network covers less than half of it.

4 A named tool now appears inside React Server Components attempts

CVE-2025-55182 is rated CVSS 10.0 and has been in CISA KEV since December 2025. Attempts eased again this period, and part of that traffic now matches a published tool. It posts to a hardcoded endpoint and ships a variant encoding the payload as UTF-16LE, which a rule written against the ASCII byte string will not match. Detect on the endpoint and request structure.

Want the full brief?

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

greynoise.io/contact

© 2026 GreyNoise, Inc.