

PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

An Adversary Tried a Citrix Zero-Day Before Disclosure

GreyNoise saw exploitation attempts on Citrix NetScaler [CVE-2026-88771](#) on 24 September, more than three days before public disclosure. Behavioral detections labeled it malicious within seconds.

3+ daysCITRIX EXPLOITATION ATTEMPTS
BEFORE PUBLIC DISCLOSURE**Over 3x**BIG-IP DISCOVERY
TRAFFIC VS PRIOR WEEK**52 of 79**CRUSHFTP BURST SOURCES THAT
ALSO TRIED CYBERPANEL**At least 4x**DAILY NEXT.JS BYPASS
SOURCES VS LATE AUGUST

WHAT'S INSIDE

New sources attempted the Citrix flaw within a day of disclosure 1

GreyNoise saw [CVE-2026-88771](#) exploitation attempts against a Swarm participant sensor on 24 September, more than three days before public disclosure. Exploitation attempts from new sources began within a day of disclosure. Read [Swarming Against Citrix 0-Day Exploitation](#).

Sources checked BIG-IP for a newly listed KEV flaw 2

CISA listed [CVE-2026-94127](#), an unauthenticated code execution flaw in the BIG-IP Access Policy Manager, in its KEV catalog with a three-day federal deadline. One of the ten sources checking for it sent about 99% of all checks. BIG-IP discovery traffic more than tripled.

Adversaries targeted CrushFTP in two single-day bursts 3

Adversaries attempted an administrator takeover flaw from 68 sources on one day, then a sandbox escape from 79 sources the next. Both sit in the KEV catalog. About two thirds of those 79 also attempted a CyberPanel flaw.

Next.js daily bypass sources ran at least 4x the August level 4

GreyNoise observed an average of 3,551 malicious sources per full day on the [Next.js middleware bypass](#), a flaw outside the KEV catalog. A payload firing alongside it arrived entirely from two large cloud and content delivery networks.

Want the full brief?

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

greynoise.io/contact