PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Four Findings, One Pattern: Systems That Hold Other Systems' Credentials

This period's four findings share one exposure pattern: each involves a system that holds credentials or files for a secondary environment, so a successful attempt against one would likely open the next without a second exploit. Exploitation attempts reached six managed file transfer products, a business intelligence platform and a web application framework inside ten days, one of them compressed into a single day.

26 of 37
SOURCES ON ONE CRUSHFTP AUTHENTICATION BYPASS, IN A SINGLE DAY

3 to 40
ANALYTICS BYPASS SOURCES, 08 TO 09 AUGUST

6 to 227
DAILY CLOUD CREDENTIAL ACCESS SOURCES, 01 TO 10 AUGUST

458 and 409
MALICIOUS SOURCES ON TWO FRAMEWORK TRAVERSAL FLAWS

WHAT'S INSIDE

1 Six file transfer products, one concentrated day

Exploitation attempts reached CrushFTP, MOVEit Transfer, GoAnywhere MFT, SolarWinds Serv-U, Wing FTP Server and Cleo, each on a CVE in CISA's Known Exploited Vulnerabilities (KEV) catalog. Of the 37 sources on one CrushFTP authentication bypass rated 9.8, 26 arrived on 02 August. Reconnaissance ran continuously underneath, at 58,237 probes against 760 exploitation attempts.

2 An analytics platform bypass, then the callbacks

Attempts to bypass the Apache Superset login rose from three sources on 08 August to 40 on 09 August. The same day, sources sending payloads built to force an outbound callback rose from a steady 11 to 20, up to 90. The flaw is a signing key Superset ships by default, so remediation is a key rotation and a restart.

3 Two framework traversal flaws moving in lockstep

Two directory traversal flaws in Next.js each drew several hundred malicious sources, 458 and 409, moving day for day: a burst on 02 August, silence by 06 August, then a restart on 07 August. Almost every source carries both signatures, so this is one population of scanners, not two campaigns.

4 Credential harvesting on three-day infrastructure

One cloud-hosted source ran credential file and cloud metadata harvesting for three days, 03 to 05 August, finished among the ten loudest sources of the period, and has not been seen since. Daily sources on cloud instance credential access climbed across the window, from 6 on 01 August to 227.

Want the full brief?

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

greynoise.io/contact