PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Adversaries Escalated Attempts on Flaws Patched Years Ago

Adversaries escalated attempts against a Spring Cloud Function code execution flaw and an Elastic Kibana file inclusion flaw from single digits to several hundred daily sources on one day. Neither had come back down when collection closed. A Sophos Firewall authentication bypass this series recorded as subsided in April returned at roughly sixty times the prior period's daily rate. Requests built to confirm whether a blind injection executed ran every day.

70x	60x	25 to 64	63%
ONE-DAY RISE IN SOURCES ON THE KIBANA FLAW	SOPHOS BYPASS RATE VS THE PRIOR PERIOD	DAILY CALLBACK SOURCES, UP FROM 11 TO 20	OF ALL DOCKER SCANNING, FROM ONE ADDRESS

WHAT'S INSIDE

1 Two flaws patched years ago jumped to several hundred sources on one day

Adversaries attempted CVE-2022-22963 in Spring Cloud Function and CVE-2018-17246 in the Elastic Kibana console on the same day. The Spring flaw is rated CVSS 9.8 and sits in CISA's Known Exploited Vulnerabilities catalog. Daily source counts on both had run in the single digits for the first six days of the period. Neither returned to that level afterward, and public exploit code exists for both.

2 A known exploited Sophos Firewall bypass returned five months after it was recorded as subsided

This series tracked the spring campaign against the CVE-2022-1040 behavior and recorded it as subsided in April. Attempts came back at roughly sixty times the prior period's daily rate, and the flaw reaches code execution on the appliance that enforces the perimeter, with no credential. Patch verification is worth more here than volume alerting. GreyNoise recorded 67 malicious sources on the flaw in the final 24 hours.

3 One host ran scans, logins and credential attacks in the same hours

A single address on a rented hosting range ran all three in the same hours. That is one tool doing all three in a single pass. That same host supplied most of the Docker Scanner activity GreyNoise observed. Corpus-wide, scanning of the manager interface outran the credential attack behavior by better than an order of magnitude. A detection keyed to failed logins therefore sees a sliver of the real pressure.

4 The daily floor on out-of-band callback sources has roughly doubled since August

Operators send these to confirm that an injected payload executed where the response itself reveals nothing. The callback behavior registered between twenty-five and sixty-four unique sources every day, with no day at zero, against eleven to twenty a day six weeks ago. The detection that matters sits outbound, in whether a server inside the estate then resolved that name.

Want the full brief?

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

greynoise.io/contact