PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Commercial Scanner Drove Log4Shell Volume

Roughly three fifths of the traffic carrying the Log4Shell exploitation tag this period came from one address range that resolves to a commercial vulnerability management service, not from an adversary. The flaws whose source populations contained nothing benign ran at two-digit volumes, well below anything a volume-ordered remediation queue surfaces. Defenders should rank on Known Exploited Vulnerabilities (KEV) listing and internet reachability instead, and resolve the operator behind an attempt figure before acting on it.

61%
OF LOG4SHELL TAG TRAFFIC FROM ONE SCANNER

~8x
MORE SOURCES SWEEP TOOLSHELL THAN EXPLOIT

100%
GEOSERVER XML EXTERNAL ENTITY SOURCES CLASSED MALICIOUS

1 day
BOTH SD-WAN KNOWN EXPLOITED BURSTS, THEN NEAR SILENCE

WHAT'S INSIDE

1 One address range carried most of the Log4Shell tag volume

Log4Shell, CVE-2021-44228, still draws heavy traffic. This period, 61% of the attempts carrying its exploitation tag came from a single range that resolves to a commercial vulnerability management service. The same range supplied 35% of generic cross-site scripting request volume and 26% of double URL encoding volume, but only 1% of broad signatures such as Generic Sensitive File Access Attempt. Inflation is worst where a flaw is most famous.

2 Sources are sweeping SharePoint farms for the ToolShell web shell

Roughly eight times more sources spent this period checking whether SharePoint farms already carry the ToolShell web shell than attempting the exploit itself. They did so on every one of the seven days. A patch closes the route in; it does not remove a shell already written. Organizations that patched in July and closed the ticket should reopen it as an artifact hunt.

3 Two SD-WAN management flaws, one single day

Adversaries attempted flaws in Cisco Catalyst SD-WAN Manager and Citrix NetScaler SD-WAN on 17 August. Both are in CISA's KEV catalog and were disclosed nine years apart. Each burst lasted one day and neither source set contained a benign member. A controller sits above every branch site it configures. Build detection on first sighting of the request path rather than on a rate threshold.

4 GeoServer discovery ran ahead of the attempts

Adversaries attempted a known exploited GeoServer XML external entity flaw across the final three days of the period. They ran at 12, 16 and 7 sources on 21, 22 and 23 August, every one classified malicious. Discovery traffic against the same product ran far heavier and across the whole window. That gap between discovery and exploitation is the warning time a patch cycle has to beat.

Want the full brief?

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

greynoise.io/contact