PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Commodity Crawlers Now Carry AI Platform Exploits

Adversaries attempted two known exploited remote code execution flaws in the AI application platform Langflow from addresses that also collected environment files and enumerated WordPress installations. Four hosts on consumer and carrier networks carried more than a third of all alternative-port SSH crawling, and one address carried more than half of the Remote Desktop crawling GreyNoise observed. Patch Langflow and rank sources by volume.

95%
OF LANGFLOW FLAW SOURCES, FROM TWO HOSTING PROVIDERS

36%
OF ALTERNATIVE-PORT SSH CRAWLING, FROM FOUR HOSTS

56%
OF ALL RDP CRAWLING, FROM ONE ADDRESS

WHAT'S INSIDE

1 Two known exploited Langflow flaws arrived inside a commodity crawler sweep

Adversaries attempted CVE-2025-3248 and CVE-2026-0770 in Langflow, both in CISA's Known Exploited Vulnerabilities catalog, at 3,968 and 4,770 connection attempts and both new to this brief series. Every address GreyNoise recorded on either flaw also carries a generic web crawling tag, roughly nine in ten collected environment files and enumerated WordPress installations, and about four in five requested repository configuration. Two hosting providers supply roughly 95% of those addresses, so the source count measures provider egress.

2 Adversaries swept SSH from consumer and carrier networks

Five of the ten highest-volume sources this period ran SSH enumeration and credential attacks, and GreyNoise classifies all five malicious. Four placed effectively all their SSH contact on ports other than 22, 36% of all alternative-port SSH crawling observed. Two shared client fingerprints group those four across four separate networks, marking a common tool class. Reputation policy scoped to hosting providers does not reach them.

3 One address supplied more than half of all Remote Desktop crawling observed

That address supplied 56% of all Remote Desktop crawling GreyNoise observed and three fifths of the credential attempts inside it. Those attempts ran 3.6% of what that source sent, so a detection keyed to failed logins sees a fraction of the pressure.