PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Edge Systems Targeted. SD-WAN Flaw Attempted in One Day.

Adversaries went after the systems that route and admit traffic into a network. They attempted a known exploited Cisco SD-WAN Manager admin bypass in a one-day burst, and three matching hosting ranges drove Sophos Firewall exploitation attempts. Cisco VPN password attempts surged for the third time in a month.

~3x	90%	1.9x	82%
SD-WAN BYPASS IPS IN ONE DAY VS REST OF WEEK	SOPHOS EXPLOIT ATTEMPTS FROM THREE RANGES	CISCO VPN PASSWORD IPS VS 22 OCTOBER PEAK	CISCO CREDENTIAL ATTEMPTS FROM FOUR HOSTS

WHAT'S INSIDE

1 A Cisco SD-WAN admin bypass in one day

Cisco SD-WAN Manager CVE-2026-76504 Auth Bypass Attempt peaked at 20 malicious IPs in a single day, with almost no discovery traffic first. CISA's fix deadline had passed a month earlier.

2 Citrix SD-WAN followed the same shape

Four days later, 24 malicious IPs attempted Citrix NetScaler Command Injection CVE-2017-6316 Attempt in a separate one-day burst, after five quiet days. Both flaws are on CISA's known exploited list.

3 Three matching ranges drove Sophos exploit attempts

Three hosting ranges on three networks sent 90% of Sophos Firewall CVE-2022-1040 Remote Code Execution Attempt traffic in near-equal shares. Blocking any one range leaves at least two thirds in place.

4 Cisco VPN password attempts surged again

Cisco SSL VPN Bruteforcer peaked at 350 malicious IPs in a day, 1.9 times the 22 October peak, its third spike in a month. Four hosting IPs sent 82% of the credential attempts.

Want the full brief?

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

greynoise.io/contact

© 2026 GreyNoise, Inc.