PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

OpenSSH Flaw Exploited on GreyNoise Sensors About 40 Hours After Its Fix. Sophos and Cisco Fleets Keep Climbing.

Adversaries exploited a new OpenSSH flaw on GreyNoise sensors. Hosting-based fleets also stepped up firewall exploitation attempts and VPN password guessing.

About 40 hours
FROM THE OPENSSH FIX TO THE FIRST EXPLOITATION OF A GREYNOISE SENSOR

+49%
SOPHOS EXPLOIT ATTEMPTS FROM THREE RANGES

Ten hosts
CISCO VPN PASSWORD FLEET, FIVE NEW TO THIS SERIES

One day
FIVE ASUS ROUTER FLAWS, NO OTHER DAY THIS WEEK

WHAT'S INSIDE

1 OpenSSH flaw exploited within two days of its fix

A new OpenSSH authentication bypass is now known exploited. Adversaries exploited it on GreyNoise sensors about 40 hours after its fix. GreyNoise captured them adding SSH keys and staging a remote control implant.

2 Sophos exploit attempts climb again

For the second brief running, three hosting ranges sent nine in ten Sophos Firewall exploitation attempts on a known exploited flaw. They raised those attempts by about half. Hosts in all three ranges carry the same client fingerprint.

3 Cisco VPN password fleet grows to ten hosts

Cisco SSL VPN Bruteforcer credential attempts rose by about a third, the third rise in a row. Hosts new to the series carried the increase. Blocking last week's hosts would miss more than half of the attempts.

4 Five ASUS router flaws in one day

On a single day, 16 or 17 malicious IPs attempted each of five ASUS RT-AX55 command injection flaws, one of them known exploited. None did on any other day of the week.

Want the full brief?

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

greynoise.io/contact

© 2026 GreyNoise, Inc.