Spike in Fortinet VPN brute-force attacks raises zero-day concerns

Data: 2025-08-13 17:49:41

Autor: Inteligência Against Invaders

A massive spike in brute-force attacks targeted Fortinet SSL VPNs earlier this month, followed by a switch to FortiManager, marked a deliberate shift in targeting that has historically preceded new vulnerability disclosures.

The campaign, detected by threat monitoring platform GreyNoise, manifested in two waves, on August 3 and August 5, with the second wave pivoting to FortiManager targeting with a different TCP signature.

As GreyNoise previously reported, such spikes in deliberate scanning and brute-forcing precede the disclosure of new security vulnerabilities 80% of the time.

Often, such scans aim at enumerating exposed endpoints, evaluating their significance, and estimating their exploitation potential, with actual attack waves following shortly after.

“New research shows spikes like this often precede the disclosure of new vulnerabilities affecting the same vendor — most within six weeks,” warned GreyNoise.

“In fact, GreyNoise found that spikes in activity triggering this exact tag are significantly correlated with future disclosed vulnerabilities in Fortinet products.”

Due to this, defenders shouldn’t dismiss those spikes in activity as failed attempts to exploit old, patched flaws, but rather treat them as potential precursors to zero-day disclosure and strengthen security measures to block them.

The Fortinet brute-force attacks

On August 3, 2025, GreyNoise recorded a spike in brute-forcing attempts targeting Fortinet SSL VPN as part of a steady activity it has been monitoring since earlier.

JA4+ fingerprint analysis,a network fingerprinting method for identifying and classifying encrypted traffic, linked the spike to June activity originating from a FortiGate device on a residential IP address associated with Pilot Fiber Inc.

“This overlap doesn’t confirm attribution, but it suggests possible reuse of tooling or network environments,” commented GreyNoise in its bulletin.

[IMAGEM REMOVIDA]FortiOS profile, traffic fingerprinted with TCP and client signatures — a meta signature — from August 5 onward was not hitting*FortiOS*," explained GreyNoise.

"Instead, it was consistently targeting our*FortiManager – FGFM* profile albeit still triggering our Fortinet SSL VPN Bruteforcer tag."

This shift suggested that either the same attackers or the same toolset/infrastructure moved from trying to brute-force VPN logins to trying to brute-force FortiManager access.

The IP addresses associated with this activity, and which should be placed on blocklists, are:

- 31.206.51.194
- 23.120.100.230
- 96.67.212.83
- 104.129.137.162
- 118.97.151.34
- 180.254.147.16
- 20.207.197.237
- 180.254.155.227
- 185.77.225.174
- 45.227.254.113

GreyNoise notes that the tracked malicious activity is evolving with time and is associated with a specific origin cluster that most likely performs adaptive testing.

In general, this activity is unlikely to be researcher scans, which are typically broader in scope and limited in rate, and wouldn't involve credential brute-forcing, which is seen as an apparent intrusion attempt.

Hence, defenders should block the listed IPs, increase login protection on Fortinet devices, and harden external access where possible, restricting access only to trusted IP ranges and VPNs.

[IMAGEM REMOVIDA]