Fortinet Warns Exploit Code Available for Critical Vulnerability - Against In

Data: 2025-08-15 04:45:06

Autor: Inteligência Against Invaders

Sysadmins have been urged to prioritize updating a new critical vulnerability in Fortinet's FortiSIEM

solution, as exploit code is currently circulating in the wild.

Published on Tuesday, CVE-2025-25256 is an escalation of privilege vulnerability with a CVSS score of 9.8.

"An improper neutralization of special elements used in an OS command vulnerability in FortiSIEM may allow an unauthenticated attacker to execute unauthorized code or commands via crafted CLI requests," the advisory explained.

"Practical exploit code for this vulnerability was found in the wild."

Fortinet added that the exploitation code currently circulating "does not appear to produce distinctive IoCs [indicators of compromise]," which will complicate network defender efforts to identify and contain any resulting exploits.

Read more on Fortinet threats: Fortinet Confirms Critical Zero-Day Vulnerability in Firewalls

FortiSIEM is a security information and event management (SIEM) platform designed to provide security operations (SecOps) teams with threat alerts based on analysis and correlation of data from multiple sources.

It's marketed mainly to medium and large enterprises and managed service providers, putting these organizations in the crosshairs of possible attack if workable exploits are developed.

Fortinet products are a popular target for threat actors, with vulnerabilitiesoften exploited in ransomware campaigns.

It's unclear whether the announcement is related to a report from GreyNoise, also released on Tuesday, which revealed a "significant spike in brute-force traffic targeting Fortinet SSL VPNs."

Over 780 unique IPswere involved in the attacks, traced to August 3. GreyNoise said this was thehighest volume of IPs associated with attacks on Fortinet SSL VPNs in recent months.

"New research shows spikes like this often precede the disclosure of new vulnerabilities affecting the same vendor – most within six weeks," it explained.

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

On August 5, the same threat actor switched from targeting FortiOS SSL VPN endpoints to FortiManager’s FGFM service, the threat intelligence firm said.