2025-04-14 - News Report

# Fortinet Warns Attackers Retain FortiGate Access Post-Patching via SSL-VPN Symlink Exploit

Summary:  
 Threat actors have found a way to maintain read-only access to vulnerable FortiGate devices. The attackers are believed to have leveraged known and now-patched security flaws. Fortinet said the modifications took place in the user file system and managed to evade detection. It's not clear who is behind the activity, but Fortinet says its investigation indicated that it was not aimed at any specific region or industry. The U.S. Cybersecurity and Infrastructure Security Agency has issued an advisory of its own. Follow us on Twitter  and LinkedIn to read more exclusive content we post. Follow us on Facebook and Twitter for updates on our latest projects and keep up to date with our latest stories. Back to the page you came from. Share your photos and videos with us on our social media channels. We would like to hear from you about your experiences. Send them to: mailonlinepictures@dailymail.co.uk and we'll feature the best in our next story. For confidential support call the Samaritans in the UK on 08457 90 90 90, visit a local Samaritans branch or click here.

Extracted Important Information:

* CVE: CVE-2022-42475
* CVE: CVE-2023-27997
* CVE: CVE-2024-21762

Link: https://thehackernews.com/2025/04/fortinet-warns-attackers-retain.html