An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2504110151

NCSC Advisory

New Post-Exploitation Technique for Known Fortinet FortiGate Vulnerabilities

17th, April 2025

STATUS: TLP:CLEAR

Description

Published: 2025-04-11

Vendor: Fortinet

Product: Relates to previously exploited Fortinet vulnerabilities within FortiGate products.

A threat actor was observed creating a malicious file from previously exploited Fortinet vulnerabilities (CVE-2024-21762, CVE-2023-27997, and CVE-2022-42475) within Fortigate products to establish read-only access to susceptible FortiGate devices.

This was accomplished by creating a symbolic link between the user filesystem and the root filesystem within a directory designated for serving SSL-VPN language files. As the modification occurred within the user filesystem, it was able to evade detection mechanisms.

Consequently, even if the device was subsequently updated to FortiOS versions that addressed the original vulnerabilities, the symbolic link may persist, enabling the threat actor to maintain read-only access to the device's file system, potentially exposing configuration files and other sensitive data.

Importantly, customers who have never enabled SSL-VPN functionality are not affected by this issue.

Products Affected

All FortiGates and FortiOS firware versions.

Impact

This malicious file could enable read-only access to files on the device's file system, which may include configurations.

Common Weakness Enumeration (CWE)[1]: N/A

Known Exploited Vulnerability (KEV) catalog[2]: Yes

Used by Ransomware Operators: Yes

[1] https://cwe.mitre.org

[2] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Fortinet.

If you detect any signs of compromise on your device, we would encourage you to contact the NCSC at the following address: certreport@ncsc.gov.ie

The following recommended steps from Fortinet should be followed:

- Upgrade all devices to 7.6.2, 7.4.7, 7.2.11 & 7.0.17 or 6.4.16.
- Review the configuration of all devices.
- Treat all configurations as potentially compromised and follow the recommended steps below to recover.

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Recommended-steps-to-execute-in-case-of-a/ta-p/230694

https://www.cisa.gov/news-events/alerts/2025/04/11/fortinet-releases-advisory-new-post-exploitation-technique-known-vulnerabilities

https://www.fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-activity