GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

28 July 2026

Advisory 174: Fortinet FortiOS SSL-VPN Symlink Persistence Patch Bypass (CVE-2025-68686).

Release Date: 27th July 2026
Impact: MEDIUM
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

Fortinet FortiOS SSL-VPN contains an Exposure of Sensitive Information to an Unauthorized Actor vulnerability (CWE-200), officially titled "SSL-VPN Symlink Persistence Patch Bypass" (FortiGuard advisory FG-IR-25-934), which may allow a remote, unauthenticated attacker to bypass the patch Fortinet previously developed for a symbolic-link persistence mechanism observed in earlier post-exploitation cases, via crafted HTTP requests.

Devices that never had SSL-VPN enabled are not affected by this issue.

What are the systems affected?

The vulnerability affects Fortinet FortiOS with SSL-VPN enabled, across the following versions:

- FortiOS 7.6.0 through 7.6.1 - Solution: upgrade to 7.6.2 or above
- FortiOS 7.4.0 through 7.4.6 - Solution: upgrade to 7.4.7 or above

- FortiOS 7.2, all versions - Solution: migrate to a fixed release
- FortiOS 7.0, all versions - Solution: migrate to a fixed release
- FortiOS 6.4, all versions - Solution: migrate to a fixed release

What does this mean?

Background - the persistence technique this patch bypasses:

- Fortinet previously identified that threat actors who had already compromised a FortiGate device via a known vulnerability (such as CVE-2022-42475, CVE-2023-27997, or CVE-2024-21762) were creating symbolic links on the device's file system to retain read-only access to sensitive files even after the initial vulnerability was patched or the device was upgraded.
- Fortinet released a patch to detect and block this specific symlink persistence mechanism.
- CVE-2025-68686 is a bypass of that specific patch: an unauthenticated attacker can send crafted HTTP requests to the SSL-VPN interface that circumvent the symlink-blocking logic, allowing continued unauthorized read access to sensitive information on a device that was already compromised at the file-system level.

In practice, this means an organisation cannot rely on the earlier Fortinet patch alone to have fully evicted an attacker who previously planted a symlink backdoor on their FortiGate device; a device that appears "patched" against the original persistence mechanism may still be leaking sensitive files to that attacker via this bypass.

Mitigation process

CERTVU recommends the following:

- Apply Fortinet's security update for CVE-2025-68686 immediately: upgrade to FortiOS 7.6.2 or above, or FortiOS 7.4.7 or above. Devices on FortiOS 7.2, 7.0, or 6.4 have no in-branch fix and should be migrated to a supported, fixed release using Fortinet's upgrade path tool (https://docs.fortinet.com/upgrade-tool).
- Because this vulnerability is only exploitable following a prior file-system-level compromise, treat any affected device as a potential indicator of an earlier, separate intrusion. Review the device for signs of prior exploitation of known FortiOS SSL-VPN RCEs (e.g. CVE-2022-42475, CVE-2023-27997, CVE-2024-21762) and for unexpected symbolic links on the file system, in addition to applying this patch.
- Where SSL-VPN is not required, disable it to remove this attack surface entirely - devices that never had SSL-VPN enabled are not affected by this vulnerability.
- Where immediate patching is not possible, Fortinet has published a virtual patch (FG-VD-60389.0day) via FortiGuard IPS/FMWP database update 26.033 - CERTVU recommends enabling this as an interim compensating control.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-68686
3. https://fortiguard.fortinet.com/psirt/FG-IR-25-934
4. https://cwe.mitre.org/data/definitions/200.html
5. https://docs.fortinet.com/upgrade-tool