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

21 October 2026

Advisory 361: Fortinet FortiOS, FortiProxy, FortiPAM and FortiSwitchManager CLI Path Traversal Vulnerability - Reported Exploited (CVE-2025-61624).

Release Date: 16th October 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 product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2025-61624 is a path traversal vulnerability (CWE-22) in the command line interpreter (CLI) of Fortinet FortiOS, FortiProxy, FortiPAM and FortiSwitchManager, published by Fortinet on 14 April 2026 as advisory FG-IR-26-122. A privileged, authenticated attacker can pass crafted path traversal sequences in the arguments of existing CLI commands to write or delete arbitrary files on the device. Fortinet found the issue internally.

What are the systems affected?

The following Fortinet product versions are affected:

- FortiOS 7.6.0 to 7.6.4 and 7.4.0 to 7.4.9, and all versions of FortiOS 7.2, 7.0 and 6.4
- FortiProxy 7.6.0 to 7.6.4 and 7.4.0 to 7.4.11, and all versions of FortiProxy 7.2 and 7.0
- FortiPAM 1.7.0, and all versions of FortiPAM 1.0 to 1.6 (FortiPAM 1.8 is not affected)
- FortiSwitchManager 7.2.0 to 7.2.7 and 7.0.0 to 7.0.6

Not affected / patched version:

- FortiOS 7.6.5 or later, or 7.4.10 or later; FortiOS 7.2, 7.0 and 6.4 have no fix and must migrate to a fixed release

- FortiProxy 7.6.5 or later, or 7.4.12 or later; FortiProxy 7.2 and 7.0 must migrate to a fixed release
- FortiPAM 1.7.1 or later; FortiPAM 1.0 to 1.6 must migrate to a fixed release
- FortiSwitchManager 7.2.8 or later, or 7.0.7 or later

What does this mean?

Successful exploitation may allow attackers to:

- Write or overwrite arbitrary files on the device after logging in as an administrator, for example to plant malicious configuration or a backdoor
- Delete arbitrary files, causing a denial of service or removing evidence
- Escalate privileges on the device and use a compromised firewall, proxy or access manager as a foothold into the network

Mitigation process

CERTVU recommends the following:

1. Upgrade to a fixed release
Upgrade each affected device to the fixed version for its branch. Devices on FortiOS 7.2, 7.0 or 6.4, FortiProxy 7.2 or 7.0, and FortiPAM before 1.7 have no direct fix and must be migrated to a supported fixed release, using Fortinet's upgrade path tool.

2. Use the virtual patch if you cannot upgrade immediately
Fortinet provides the virtual patch FG-VD-59270.0day in FMWP database update 25.120. This is a temporary measure and does not replace upgrading. Tenable Nessus plugin 306463 can detect affected devices.

3. Restrict administrative access

4. Review for compromise

Report suspected compromise to CERTVU.

Reference

1. https://fortiguard.fortinet.com/psirt/FG-IR-26-122
2. https://nvd.nist.gov/vuln/detail/CVE-2025-61624
3. https://www.tenable.com/plugins/nessus/306463
4. https://www.wiz.io/vulnerability-database/cve/cve-2025-61624
5. https://www.cisa.gov/known-exploited-vulnerabilities-catalog