

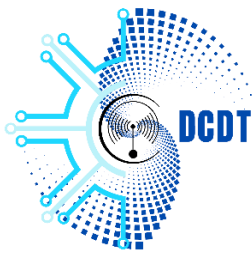
**GOVERNMENT OF THE REPUBLIC  
OF VANUATU**

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

10 September 2026

**Advisory 285: Fortinet FortiOS and FortiSwitchManager CAPWAP Daemon  
Heap-Based Buffer Overflow - Actively Exploited via PivotC2 RAT (CVE-2025-  
25249).**

**Release Date:** 9<sup>th</sup> September 2026

**Impact:** **CRITICAL**

**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 operate a Fortinet FortiGate firewall or FortiSwitchManager. This alert is intended to be understood by technical users and systems administrators, and requires urgent action given confirmed, large-scale active exploitation.

## What is it?

CVE-2025-25249 is a critical heap-based buffer overflow in the cw\_acd daemon of FortiOS and FortiSwitchManager, which handles CAPWAP (Control and Provisioning of Wireless Access Points) traffic on UDP port 5246. An unauthenticated remote attacker can send specially crafted CAPWAP packets to trigger the overflow and execute arbitrary code on the affected appliance, with no credentials or user interaction required.

## What are the systems affected?

The following version(s) are affected:

- FortiOS 6.4 (all versions), 7.0.0–7.0.17, 7.2.0–7.2.11, 7.4.0–7.4.8, and 7.6.0–7.6.3 - (Affected)
- FortiSwitchManager 7.0.0–7.0.5 and 7.2.0–7.2.6 - (Affected)

FortiOS 6.4.17+, 7.0.18+, 7.2.12+, 7.4.9+, 7.6.4+, and FortiSwitchManager 7.0.6+/7.2.7+ is not affected – (Patched)

## What does this mean?

### Typical attack flow:

1. **Reach the exposed CAPWAP service**
  - An unauthenticated remote attacker sends specially crafted CAPWAP packets to the cw\_acd daemon on UDP port 5246 of a FortiGate or FortiSwitchManager appliance that has the fabric/wireless-controller service reachable on an external or WAN-facing interface.
2. **Trigger the overflow and deploy the PivotC2 RAT**
  - The crafted packet triggers the heap overflow and achieves code execution, which the observed campaign uses to run a self-extracting exploit chain ("fortirun.bin"), establish a reverse shell, and download and install the PivotC2 remote access trojan — providing the attacker persistent access, automated credential/configuration harvesting, and SOCKS5/HTTP proxy tunnelling through the compromised appliance.

### Attack vectors:

- A network-based, unauthenticated attack against any FortiGate or FortiSwitchManager appliance with the CAPWAP/fabric service reachable from an untrusted network, most commonly the public internet.
- No user interaction or privileges are required (CVSS AV:N/PR:N/UI:N).

Successful exploitation may allow attackers to:

- Gain full, persistent remote access to the firewall or wireless-controller appliance itself, typically one of the most trusted devices on a network - via the PivotC2 remote access trojan.
- Automatically harvest and decrypt stored credentials and secrets from the appliance's configuration (VPN pre-shared keys, SSL-VPN, LDAP, and administrative accounts), and use the compromised device as a proxy or pivot point to reach, exfiltrate from, or further compromise the internal network behind it.

## Mitigation process

CERTVU recommends the following:

### 1. Apply the vendor patch without delay

- Update to FortiOS 7.6.4+, 7.4.9+, 7.2.12+, 7.0.18+, or 6.4.17+, or FortiSwitchManager 7.2.7+/7.0.6+ as applicable, per Fortinet PSIRT advisory FG-IR-25-084.

2. Restrict exposure of the CAPWAP/fabric service as defence-in-depth
3. Treat this as a likely-compromise scenario, not just a patch-and-move-on situation
4. Rotate all credentials and secrets after patching

Report any suspected compromise of a Fortinet FortiGate or FortiSwitchManager appliance to CERTVU at [incident@cert.gov.vu](mailto:incident@cert.gov.vu) or on telephone (678) 33380.

## Reference

1. <https://www.fortiguard.com/psirt/FG-IR-25-084>
2. <https://nvd.nist.gov/vuln/detail/CVE-2025-25249>
3. <https://socradar.io/blog/cve-2025-25249-pivotc2-fortigate-rat/>