

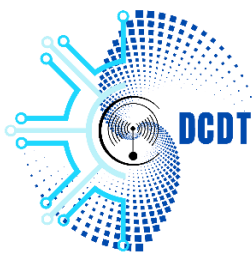
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

15 October 2026

**Advisory 358: Palo Alto Networks PAN-OS Management Interface Code
Injection Vulnerability - Actively Exploited (CVE-2026-0322).**

Release Date: 14th October 2026

Impact: **HIGH**

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-2026-0322 is a code injection vulnerability (CWE-94) in the management interface of Palo Alto Networks PAN-OS. An attacker who is authenticated to the management interface and can reach it over the network can run arbitrary code with root privileges on the firewall. It is rated CVSS v4.0 8.6 (High). No special configuration is needed, but the risk is highest where the management interface is reachable from the internet, and because the flaw needs valid administrator credentials, stolen or weak credentials make it easier to use.

What are the systems affected?

The following PAN-OS versions are affected on PA-Series and VM-Series firewalls and on Panorama (virtual appliances and M-Series):

- PAN-OS 12.2 before 12.2.4
- PAN-OS 12.1 before 12.1.10-h2
- PAN-OS 11.2 before 11.2.16
- PAN-OS 11.1 before 11.1.16-h3
- PAN-OS 10.2 before 10.2.18-h12

Not affected / patched version:

- PAN-OS 12.2.4, 12.1.10-h2, 11.2.16, 11.1.16-h3 or 10.2.18-h12 or later, as applicable. Older minor releases have their own hotfix builds listed in the vendor advisory, and unsupported releases must be migrated. Cloud NGFW and Prisma Access are not affected

What does this mean?

Successful exploitation may allow attackers to:

- Run commands as root on the firewall or Panorama after logging in to the management interface, taking full control of the device
- Change firewall rules, intercept or redirect traffic, and steal VPN and administrator credentials and configuration secrets
- Use the compromised firewall or Panorama, which manages many firewalls, as a foothold into the network

Mitigation process

CERTVU recommends the following:

1. Patch to the fixed release

Upgrade each firewall and Panorama to the fixed build for its branch. Palo Alto Networks states there is no complete workaround, so patching is the remediation.

2. Lock down management access

Do not expose the management interface to the internet. Restrict it to a hardened jump box or trusted administrator IP addresses and use multi-factor authentication. This reduces the exposure but does not fix the flaw.

3. Use Threat Prevention signatures as partial cover

4. Hunt for compromise

5. Rotate credentials

Reference

1. <https://security.paloaltonetworks.com/CVE-2026-0322>
2. <https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-pan-os-rce-flaw-exploited-in-attacks/>
3. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
4. <https://nvd.nist.gov/vuln/detail/CVE-2026-0322>