مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Palo Alto Networks PAN-OS

Tracking #:432318902

Date:06-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Palo Alto Networks PAN-OS, tracked as CVE-2026-0300, affecting the User-ID Authentication Portal (Captive Portal) service on PA-Series and VM-Series firewalls. This vulnerability is actively exploited in the wild and allows unauthenticated remote attackers to execute arbitrary code with root privileges through specially crafted packets.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-0300**
- **Severity:** Critical | **CVSS:** 9.3
- A buffer overflow vulnerability exists in the User-ID Authentication Portal (Captive Portal) service of Palo Alto Networks PAN-OS. An unauthenticated remote attacker can exploit this flaw by sending specially crafted packets to vulnerable firewalls, resulting in arbitrary code execution with root privileges.
- Internet-exposed Captive Portal deployments are at greatest risk. Palo Alto Networks has confirmed limited in-the-wild exploitation targeting exposed systems.
- Successful exploitation could lead to full firewall compromise, traffic interception, security control bypass, and unauthorized access to internal enterprise networks.

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.4-h5 < 12.1.7	>= 12.1.4-h5 (ETA: 05/13) >= 12.1.7 (ETA: 05/28)
PAN-OS 11.2	< 11.2.4-h17 < 11.2.7-h13 < 11.2.10-h6 < 11.2.12	>= 11.2.4-h17 (ETA: 05/28) >= 11.2.7-h13 (ETA: 05/13) >= 11.2.10-h6 (ETA: 05/13) >= 11.2.12 (ETA: 05/28)
PAN-OS 11.1	< 11.1.4-h33 < 11.1.6-h32 < 11.1.7-h6 < 11.1.10-h25 < 11.1.13-h5 < 11.1.15	>= 11.1.4-h33 (ETA: 05/13) >= 11.1.6-h32 (ETA: 05/13) >= 11.1.7-h6 (ETA: 05/28) >= 11.1.10-h25 (ETA: 05/13) >= 11.1.13-h5 (ETA: 05/13) >= 11.1.15 (ETA: 05/28)

PAN-OS 10.2	< 10.2.7-h34 < 10.2.10-h36 < 10.2.13-h21 < 10.2.16-h7 < 10.2.18-h6	>= 10.2.7-h34 (ETA: 05/28) >= 10.2.10-h36 (ETA: 05/13) >= 10.2.13-h21 (ETA: 05/28) >= 10.2.16-h7 (ETA: 05/28) >= 10.2.18-h6 (ETA: 05/13)
Prisma Access	None	All

Fixed Versions
Palo Alto Networks is releasing patches across supported PAN-OS branches according to published ETA schedules.

Immediate Mitigations

- Restrict User-ID Authentication Portal access to trusted internal IP addresses only
- Block portal exposure from the public internet or untrusted zones
- Disable User-ID Authentication Portal if not operationally required
- Apply Threat Prevention Signature updates (available for PAN-OS 11.1+)
- Review Device > User Identification > Authentication Portal Settings to confirm exposure status

RECOMMENDATIONS:

- Immediately identify whether User-ID Authentication Portal is enabled
- Upgrade to the appropriate fixed PAN-OS release as soon as available
- Prioritize patching internet-facing or externally accessible devices
- Restrict management and authentication interfaces to internal networks
- Monitor firewall logs for suspicious portal traffic or exploitation attempts
- Deploy Threat Prevention signatures as soon as available
- Review firewall configurations to minimize unnecessary external exposure

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://security.paloaltonetworks.com/CVE-2026-0300