CERT-EU

Security Advisory 2026-006

Critical Vulnerability in PAN-OS

2026-05-06 — v1.0

TLP:CLEAR

History:

- *06/05/2026 — v1.0 – Initial publication*

Summary

On 6 May 2026, Palo Alto published a security advisory addressing a critical vulnerability affecting PAN-OS [1]. This vulnerability allows an unauthenticated attacker to execute arbitrary code with root privileges.

Palo Alto observed limited exploitation of this vulnerability. It is strongly recommended updating affected appliances as soon as patches will be available, and to apply workarounds and mitigation in the meantime.

Technical Details

The vulnerability **CVE-2026-0300**, with the CVSS score of 9.3, is a buffer overflow in the User-ID Authentication Portal (aka Captive Portal) service of Palo Alto Networks PAN-OS software. [1]

An unauthenticated attacker could execute arbitrary code with root privileges on the PA-Series and VM-Series firewalls by sending specially crafted packets. [1]

Affected Products

This issue is applicable only to PA-Series and VM-Series firewalls that are configured to use User-ID Authentication Portal.

The following PAN-OS versions are affected:

- Versions prior to 12.1.4-h5
- Versions prior to 12.1.7
- Versions prior to 11.2.4-h17
- Versions prior to 11.2.7-h13
- Versions prior to 11.2.10-h6
- Versions prior to 11.2.12
- Versions prior to 11.1.4-h33
- Versions prior to 11.1.6-h32
- Versions prior to 11.1.7-h6
- Versions prior to 11.1.10-h25

- Versions prior to 11.1.13-h5
- Versions prior to 11.1.15
- Versions prior to 10.2.7-h34
- Versions prior to 10.2.10-h36
- Versions prior to 10.2.13-h21
- Versions prior to 10.2.16-h7
- Versions prior to 10.2.18-h6

Additional information is available in the vendor's advisory [1].

Recommendations

The patches are not available at the time of writing, but are scheduled to be released in the near future. It is recommended updating affected devices as soon as the patches will be released.

Mitigation

It is possible to mitigate the risk of this flaw by taking either of the following actions [1]:

- Restrict User-ID Authentication Portal access to only trusted zones.
- Disable User-ID Authentication Portal if not required.

References

[1] https://security.paloaltonetworks.com/CVE-2026-0300