An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605070269

# NCSC Advisory

## Palo Alto Networks PAN-OS: Unauthenticated user initiated Buffer Overflow Vulnerability in User-ID Authentication Portal

CVE-2026-0300

**7th, May 2026**

**STATUS: TLP:CLEAR**

# Description

**CVE ID:** CVE-2026-0300

**Published:** 2026-05-06

**Vendor:** Palo Alto Networks

**Product:** PAN-OS

**CVSS Score[1]:** 9.3

# Products Affected

| Product | Version |
| --- | --- |
| PAN-OS 12.1 | < 12.1.4-h5<br>< 12.1.7 |
| PAN-OS 11.2 | < 11.2.4-h17<br>< 11.2.7-h13<br>< 11.2.10-h6<br>< 11.2.12 |
| PAN-OS 11.1 | < 11.1.4-h33<br>< 11.1.6-h32<br>< 11.1.7-h6<br>< 11.1.10-h25<br>< 11.1.13-h5<br>< 11.1.15 |
| PAN-OS 10.2 | < 10.2.7-h34<br>< 10.2.10-h36<br>< 10.2.13-h21<br>< 10.2.16-h7<br>< 10.2.18-h6 |

[1] https://www.first.org/cvss/

# Impact

A buffer overflow vulnerability in the User-ID™ Authentication Portal (aka Captive Portal) service of Palo Alto Networks PAN-OS software allows an unauthenticated attacker to execute arbitrary code with root privileges on the PA-Series and VM-Series firewalls by sending specially crafted packets.

The risk of this issue is greatly reduced if you secure access to the User-ID™ Authentication Portal per the best practice guidelines in recommendations section by restricting access to only trusted internal IP addresses.

Prisma Access, Cloud NGFW and Panorama appliances are **not** impacted by this vulnerability.

**Common Weakness Enumeration (CWE)[2]:** CWE-787: Out-of-bounds Write

**Known Exploited Vulnerability (KEV) catalog[3]**: Yes

**Used by Ransomware Operators**: N/A

# Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Palo Alto Networks.

- https://nvd.nist.gov/vuln/detail/CVE-2026-0300
- https://www.cve.org/CVERecord?id=CVE-2026-0300
- https://security.paloaltonetworks.com/CVE-2026-0300
- https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CqbiCAC
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-0300

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog