

CVE-2026-0300

Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability

CISA KEV since May 6, 2026

Actively exploited

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 <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail> by restricting access to

EVRS 75/₁₀₀ Urgent priority	CVSS V4.0 9.3 Critical · NVD	EPSS 0.317 98.3rd percentile · FIRST	CISA DEADLINE May 9, 2026 CISA federal deadline · Overdue by 5 months
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.317 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. Until the vendor releases an official fix, the following workaround should be implemented: - Restrict User-ID Authentication Portal access to only trusted zones. - Disable User-ID Authentication Portal if not required. 5/13/2026: Palo Alto has released a variety of patches. If these are relevant to your environment, please apply the designated patch.

Basis: CISA KEV required action

only trusted internal IP addresses. Prisma Access, Cloud NGFW and Panorama appliances are not impacted by this vulnerability.

Affected and fixed versions · 42 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
pan-os	10.2.0	no fixed version listed	NVD
	10.2.1		
	10.2.2		
	10.2.3		
	10.2.4		
	10.2.5		
	10.2.6		
	10.2.7		
	10.2.8		
	10.2.9		
	10.2.10		
	10.2.11		
	10.2.12		
	10.2.13		
	10.2.14		
	10.2.15		
	10.2.16		
	10.2.17		
	10.2.18		
	11.1.0		
	11.1.1		
	11.1.2		
	11.1.3		
	11.1.4		
	11.1.5		
	11.1.6		
	11.1.7		
	11.1.8		
	11.1.9		
	11.1.10		
	11.1.11		
	11.1.12		
	11.1.13		
	11.1.14		
	11.2.0		
	11.2.1		
	11.2.2		
	11.2.3		
	11.2.4		
	11.2.5		
	11.2.6		
	11.2.7		
	11.2.8		
	11.2.9		
	11.2.10		
	11.2.11		
	12.1.2		
	12.1.3		
	12.1.4		
	12.1.5		
	12.1.6		
ruggedcom ape1808 firmware	—	no fixed version listed	NVD
pa-1410	—	no fixed version listed	NVD
pa-1420	—	no fixed version listed	NVD
pa-3410	—	no fixed version listed	NVD
pa-3420	—	no fixed version listed	NVD
pa-3430	—	no fixed version listed	NVD
pa-3440	—	no fixed version listed	NVD



Sources

Vendor guidance github.com/advisories/GHSA-3vfh-3cpw-2378
NVD nvd.nist.gov/vuln/detail/CVE-2026-0300

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-27879

Additional guidance security.paloaltonetworks.com/CVE-2026-0300
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2026-0300

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.