Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

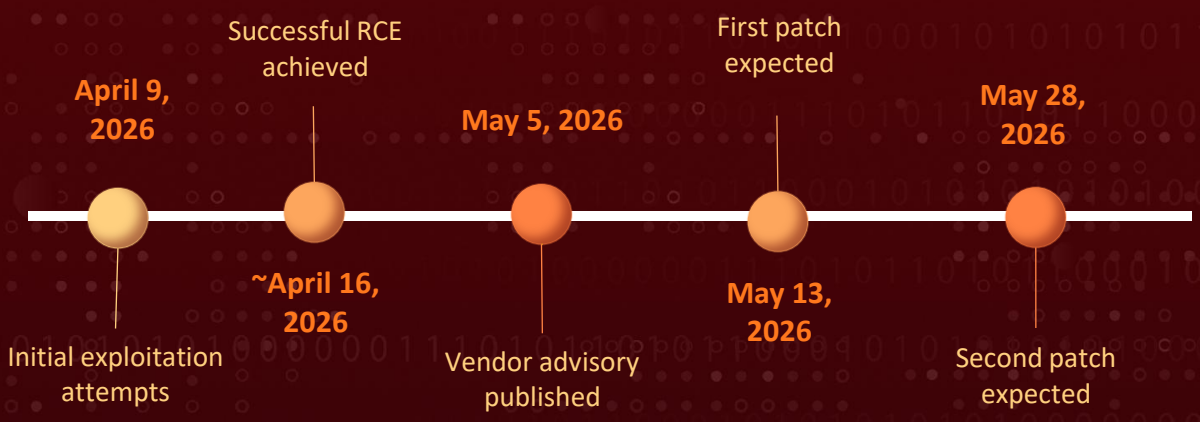
PAN-OS Buffer Overflow Flaw Under Active State-Sponsored Exploitation

Date of Publication	Admiralty Code	TA Number
May 07, 2026	A1	TA2026122

Summary

First Seen: April 09, 2026
Affected Products: Palo Alto Networks PAN-OS (PA-Series Firewalls, VM-Series Firewalls)
Threat Actor: CL-STA-1132
Malware: EarthWorm, ReverseSocks5
Impact: A critical zero-day in Palo Alto Networks PAN-OS firewalls, the very devices organizations trust to guard their perimeter, is being actively exploited by a likely state-sponsored actor tracked as CL-STA-1132. CVE-2026-0300 is a buffer overflow in the User-ID Authentication Portal that lets an unauthenticated attacker achieve root-level code execution with a single crafted packet, no credentials or user interaction required. The attacker used this foothold to inject shellcode into nginx, deploy EarthWorm and ReverseSocks5 tunneling tools, enumerate Active Directory, and methodically wipe forensic evidence, all while patches remain unavailable until May 13, 2026.

Timeline



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-0300	Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability	Palo Alto Networks PAN-OS	✓	✓	✗

Vulnerability Details

#1

CVE-2026-0300 is a buffer overflow vulnerability classified under CWE-787 (Out-of-bounds Write). The flaw resides in the User-ID Authentication Portal (Captive Portal) service in Palo Alto Networks PAN-OS software. This component maps IP addresses to user identities when the firewall cannot automatically perform this association.

#2

The root cause of the vulnerability is an out-of-bounds write condition in the Captive Portal service. When the portal processes incoming network packets, it fails to properly validate the size or boundaries of input data, allowing an attacker to overwrite adjacent memory. By sending specially crafted packets to the portal, an unauthenticated remote attacker can trigger this buffer overflow to inject and execute arbitrary code. Because the Captive Portal service runs with root privileges, successful exploitation immediately grants the attacker the highest level of access on the device.

#3

The vulnerability affects PAN-OS versions across four major branches: PAN-OS 10.2 (multiple hotfix streams prior to 10.2.7-h34, 10.2.10-h36, 10.2.13-h21, 10.2.16-h7, and 10.2.18-h6), PAN-OS 11.1 (prior to 11.1.4-h33, 11.1.6-h32, 11.1.7-h6, 11.1.10-h25, 11.1.13-h5, and 11.1.15), PAN-OS 11.2 (prior to 11.2.4-h17, 11.2.7-h13, 11.2.10-h6, and 11.2.12), and PAN-OS 12.1 (prior to 12.1.4-h5 and 12.1.7). The vulnerability is applicable only to PA-Series and VM-Series firewalls configured with the User-ID Authentication Portal enabled. Cloud NGFW, Prisma Access, and Panorama are not affected.

#4

Palo Alto Networks has confirmed limited active exploitation targeting User-ID Authentication Portals exposed to untrusted IP addresses and the public internet. The activity is attributed to CL-STA-1132, a likely state-sponsored actor. The exploitation timeline shows initial unsuccessful attempts beginning April 9, 2026, with successful remote code execution achieved approximately one week later. Post-exploitation activity included shellcode injection into nginx worker processes, deployment of EarthWorm and ReverseSocks5 tunneling tools, Active Directory enumeration via the firewall's service account credentials, and extensive log and evidence destruction. A Threat Prevention signature (Threat ID 510019) is available for customers running PAN-OS 11.1 and above with an Advanced Threat Prevention subscription.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-0300	Palo Alto Networks PAN-OS (PA-Series, VM-Series) Versions 10.2.x, 11.1.x, 11.2.x, 12.1.x	cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:*	CWE-787

Recommendations

Restrict User-ID Authentication Portal Access Immediately: Organizations should immediately restrict access to the User-ID Authentication Portal to trusted internal IP addresses only. This is the most effective mitigation available today. Follow the vendor-provided guidance in the Palo Alto Networks Knowledgebase article and Live Community article to configure zone-based access restrictions. Additionally, disable Response Pages in the Interface Management Profile attached to every L3 interface in any zone where untrusted or internet traffic can ingress, keeping Response Pages enabled only on interfaces in trust/internal zones.

Disable the Authentication Portal If Not Required: If the User-ID Authentication Portal is not actively needed for your environment's user identification workflows, disable it entirely via Device > User Identification > Authentication Portal Settings. This completely eliminates the attack surface for CVE-2026-0300 and is the simplest way to remove risk until patches are available.

Enable Threat Prevention Signature (Threat ID 510019): Customers with an Advanced Threat Prevention subscription running PAN-OS 11.1 or later should ensure Threat ID 510019 from Applications and Threats content version 9097-10022 is enabled. This signature provides network-level detection and blocking of exploitation attempts targeting CVE-2026-0300.

Apply Patches as Soon as They Are Released: Palo Alto Networks plans to release the first batch of fixes on May 13, 2026, with a second batch on May 28, 2026. Organizations should plan their patching schedule now, test patches in staging environments promptly, and deploy to production firewalls as quickly as possible. Prioritize internet-facing firewalls with the Authentication Portal enabled.

Conduct Compromise Assessment and Forensic Review: Given the confirmed exploitation by CL-STA-1132, organizations that have had the User-ID Authentication Portal exposed to the internet or untrusted networks should proactively investigate for signs of compromise. Review nginx crash logs, audit logs for ptrace injection evidence, check for unexpected files in /var/tmp/ and /tmp/ directories (e.g., linuxap, linuxda, linuxupdate, .c, R5), and look for unauthorized Active Directory enumeration activity originating from firewall service accounts.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1548: Abuse Elevation Control Mechanism	T1548.001: Setuid and Setgid
Defense Evasion	T1070: Indicator Removal	T1070.004: File Deletion
Credential Access	T1003: OS Credential Dumping	
Discovery	T1018: Remote System Discovery	
Command and Control	T1090: Proxy	
	T1572: Protocol Tunneling	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	67[.]206[.]213[.]86, 136[.]0[.]8[.]48, 146[.]70[.]100[.]69, 149[.]104[.]66[.]84
URLs	hxxp[:]//146[.]70[.]100[.]69[:]8000/php_sess, hxxps[:]//github[.]com/Acebond/ReverseSocks5/releases/download/v2.2.0/ReverseSocks5-v2.2.0-linux-amd64.tar[.]gz
SHA256	e11f69b49b6f2e829454371c31ebf86893f82a042dae3f2faf63dcd84f97a584
File Path	/var/tmp/linuxap, /var/tmp/linuxda, /var/tmp/linuxupdate, /tmp/.c, /tmp/R5, /var/R5

Patch Details

No patches are currently available for CVE-2026-0300. Palo Alto Networks has committed to releasing fixes in two phases, on May 13 and May 28, 2026. Until then, organizations should keep a close watch on the vendor's security advisory page and prepare their patching workflows in advance to minimize the window of exposure once updates drop.

References

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

https://unit42.paloaltonetworks.com/captive-portal-zero-day/

https://www.wiz.io/blog/critical-vulnerability-in-pan-os-exploited-in-the-wild-cve-2026-0300

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo of **HivePro.**

REPORT GENERATED ON

May 07, 2026 • 8:30 AM

More at www.hivepro.com