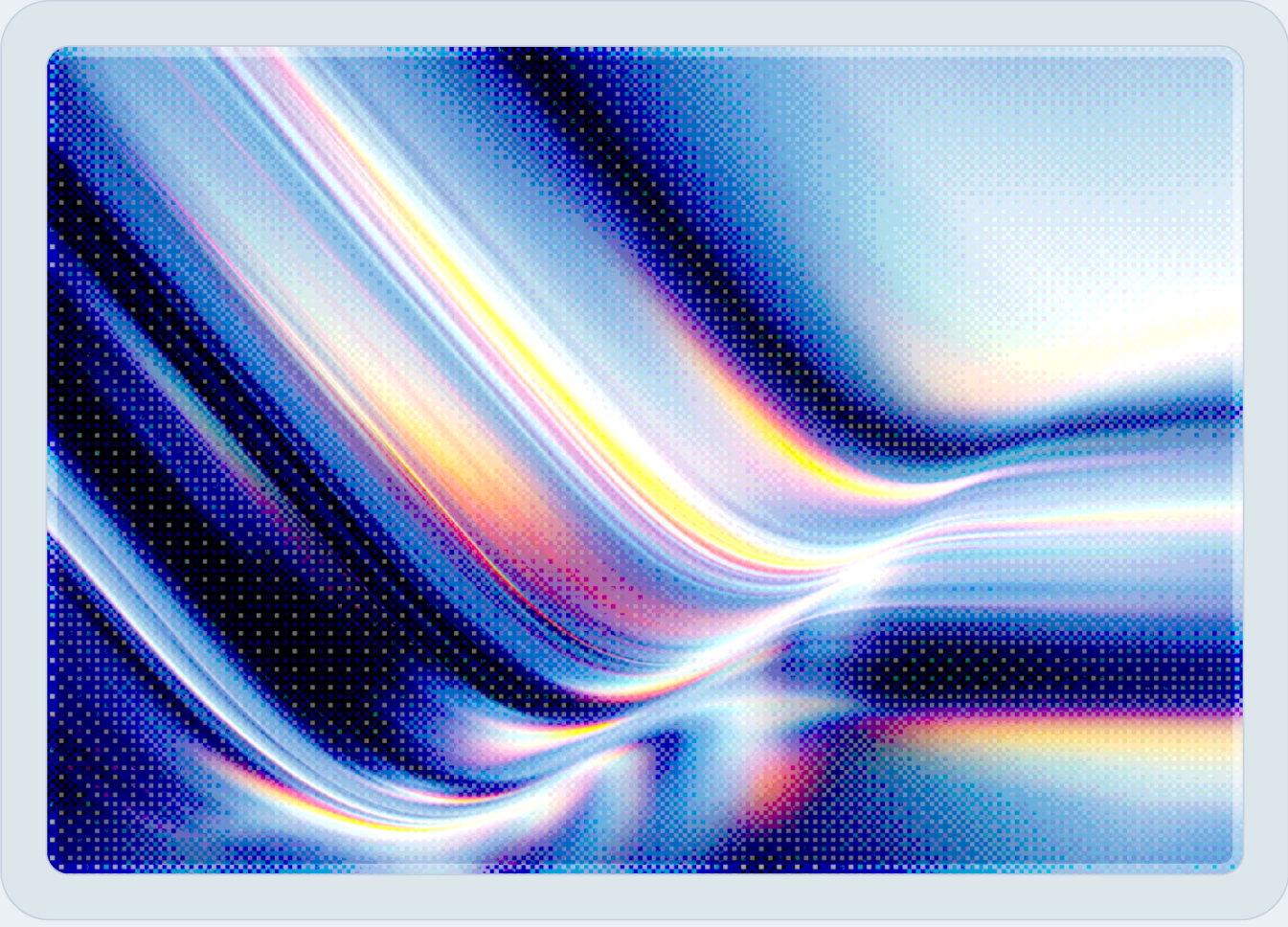
CSAI Foundation | Cloud Security Alliance

PAN-OS Captive Portal RCE: Zero-Auth Root Access Exploited

Emergency Guidance for CVE-2026-0300

2026-05-06

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

CVE-2026-0300 is a critical buffer overflow vulnerability in the Palo Alto Networks PAN-OS User-ID Authentication Portal (also referred to as the Captive Portal) that allows an unauthenticated, network-based attacker to execute arbitrary code with root-level privileges on affected PA-Series and VM-Series firewalls. The vulnerability carries a CVSS 4.0 score of 9.3 on internet-exposed configurations [1] and requires no credentials, no user interaction, and no special preconditions to exploit—characteristics that make it well-suited for automated, mass-exploitation campaigns.

- Active exploitation has been confirmed by Palo Alto Networks as of May 6, 2026, with observed attacks targeting Authentication Portal instances exposed to untrusted networks [1] [10]. Shadowserver data published at the time of disclosure identifies more than 5,800 PAN-OS VM-Series firewalls with direct internet exposure, with the largest concentrations in Asia (2,466) and North America (1,998) [6].
- Official patches are not yet available for all affected PAN-OS branches; Palo Alto Networks has announced a rolling patch schedule with releases expected between May 13 and May 28, 2026 [1][3]. This gap makes pre-patch mitigation controls—specifically access restriction and portal disablement—urgent and essential for affected organizations with internet-accessible portal configurations.
- A Threat Prevention Signature capable of detecting and blocking active exploit attempts was made available on May 5, 2026, for customers running PAN-OS 11.1 and above [1]. Organizations on earlier branches must rely on network-layer access controls until patches are available.
- The vulnerability affects PAN-OS 10.2, 11.1, 11.2, and 12.1 across PA-Series and VM-Series hardware; Prisma Access, Cloud NGFW, and Panorama are not affected [1].

Background

Palo Alto Networks is one of the largest vendors of enterprise network security appliances, and PAN-OS is the operating system running across the company's PA-Series physical firewalls, VM-Series virtualized firewalls, and CN-Series container firewalls. These appliances are widely deployed across enterprise environments including critical infrastructure, financial services, healthcare, and government sectors,

where they serve in network perimeter, data center segmentation, and hybrid cloud enforcement roles [12]. Because PAN-OS devices operate as the enforcement point for network segmentation, traffic inspection, and access policy, a successful compromise of the underlying operating system—particularly one that yields root-level code execution—represents a complete loss of the security controls those devices provide and potential lateral access to protected network segments behind the firewall.

The User-ID Authentication Portal, sometimes called the Captive Portal, is a PAN-OS feature that presents an authentication interface to end users who attempt to access network resources before their identity has been mapped to a user or group for policy enforcement. When a user connects from a new device or session, PAN-OS can redirect them to the portal to authenticate, at which point the firewall maps the user's identity to the traffic flow for policy application. This feature serves a legitimate and common enterprise purpose: ensuring that group-based security policies can be enforced dynamically as users move between devices or network segments. However, when the portal is configured to accept connections from untrusted networks—or, in the highest-risk scenario, from the public internet—the authentication surface is exposed to any unauthenticated actor capable of reaching the endpoint.

CVE-2026-0300 was publicly disclosed on May 6, 2026, through Palo Alto Networks' official security advisory [1][2][12]. The vulnerability was identified in the buffer handling logic of the User-ID Authentication Portal service and reported to Palo Alto Networks prior to the advisory's publication. The disclosure was coordinated with the simultaneous release of the Threat Prevention Signature for supported branches, and the vendor confirmed limited active exploitation at the time of disclosure. The formal patch release schedule places full remediation availability no earlier than May 13, 2026, creating an immediate window in which impacted organizations must rely on configuration-based mitigations.

Security Analysis

Vulnerability Mechanism

CVE-2026-0300 is a stack-based buffer overflow vulnerability (CWE-121) in the code path responsible for processing user-submitted requests to the PAN-OS User-ID Authentication Portal. The flaw arises from insufficient bounds checking on attacker-controlled input: when specially crafted packets are sent to the portal service, the input data overflows a fixed-size buffer on the stack, allowing an attacker to overwrite adjacent memory—including function return addresses—and redirect program execution to attacker-supplied code [3][4]. Because the portal service runs with root privileges, the code that executes through the overflowed buffer runs in the same elevated context, yielding full root-level control of the PAN-OS instance without the attacker having authenticated in any way.

The attack vector is classified as NETWORK, the attack complexity as LOW, and privileges required as NONE [1]. This combination is significant: it means the vulnerability is reachable over any network path to which the attacker has access, requires no trial-and-error or complex precondition setup, and demands no pre-existing foothold or credential. User interaction is also not required, meaning the exploit can be fired as a pure network probe without waiting for any human action on the target. These characteristics place CVE-2026-0300 in the Critical severity band—the highest CVSS 4.0 tier—for operational risk, a category where automated scanning tools can discover vulnerable endpoints within hours of public disclosure, and where the exploitation complexity is low enough to offer defenders little inherent friction advantage [4][5].

The CVSS 4.0 score drops from 9.3 to 8.7 when the portal is accessible only from trusted internal IP addresses rather than from untrusted or internet-exposed zones [1]. This scoring delta is not incidental: it reflects the real-world risk reduction achieved by restricting portal access, and it is the basis for the primary compensating control available while patches are staged.

Affected Scope and Internet Exposure

The vulnerability affects PA-Series and VM-Series firewalls running the following unpatched PAN-OS versions: PAN-OS 10.2 prior to 10.2.7-h34, 10.2.10-h36, 10.2.13-h21, 10.2.16-h7, or 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, or 11.1.15; PAN-OS 11.2 prior to 11.2.4-h17, 11.2.7-h13, 11.2.10-h6, or 11.2.12; and PAN-OS 12.1 prior to 12.1.4-h5 or 12.1.7 [1]. Prisma Access, Cloud NGFW, and Panorama are explicitly not affected.

Shadowserver's internet-wide scanning data, published concurrently with the advisory, identified more than 5,800 PAN-OS VM-Series instances with direct internet exposure [6]. While not all exposed appliances necessarily have the User-ID Authentication Portal enabled or internet-accessible, the number of reachable PAN-OS endpoints provides a rough lower bound on the population of potentially exploitable targets. Internet exposure is the highest-risk configuration; organizations with firewalls reachable directly from untrusted networks and with the portal enabled face the full 9.3 CVSS risk score.

The geographic concentration of exposed appliances—with the plurality located in Asia (2,466) and a substantial cohort in North America (1,998) [6]—indicates broad global relevance across any region with enterprise PAN-OS deployments. Organizations in any region should assess their exposure and apply mitigations regardless of perceived regional threat profiles. State-sponsored threat actors from multiple regions have demonstrated both the capability and the willingness to exploit critical network infrastructure vulnerabilities rapidly following public disclosure, as observed with prior PAN-OS vulnerabilities including CVE-2024-3400, which was exploited as a zero-day against GlobalProtect before patches were available [13][14].

Exploitation Landscape and Threat Context

Palo Alto Networks' disclosure language—"limited exploitation" observed in the wild—is the same framing the vendor used in early disclosures of CVE-2024-3400, where "limited" exploitation at disclosure time escalated to widespread opportunistic exploitation within days of proof-of-concept code becoming available [13][14]. This pattern has proven structurally predictable: high-CVSS unauthenticated RCEs against market-leading network security appliances have historically attracted rapid weaponization once the vulnerability class and triggering condition are publicly known. As has been observed with prior vulnerability disclosures, the availability of network detection signatures may also provide reverse-engineering reference points for threat actors developing reliable exploits—a recognized trade-off in coordinated vulnerability disclosure.

The consequences of a successful exploit extend well beyond the firewall device itself. An attacker achieving root-level code execution on a PAN-OS appliance gains access to the management plane of the network perimeter control point—the device that determines what traffic is permitted, inspected, or blocked across the segments it separates. From this position, an attacker can modify firewall policies to permit attacker-controlled traffic into protected networks, extract stored credentials, certificates, or VPN configuration data, disable or tamper with security inspection functions, and use the firewall's privileged network position to pivot laterally into segments that are otherwise isolated [4][5][8][11]. For organizations where PAN-OS appliances enforce segmentation between corporate and industrial networks, between sensitive data environments and general user segments, or between cloud workloads and on-premises infrastructure, the blast radius of a single exploited firewall can extend across the protected systems behind it, depending on the depth of downstream segmentation and endpoint defenses in place.

Recommendations

Actions in this section are sequenced by urgency: Immediate Actions should be completed within 24 hours of this advisory; Short-Term Mitigations apply throughout the patch window through May 28; Strategic Considerations address ongoing program improvements that this incident should motivate.

Immediate Actions

The foundational action—without which other mitigations cannot be consistently applied—is identifying all PAN-OS appliances in the environment and determining which have the User-ID Authentication Portal enabled. Administrators should review the Security Policy and Network > Zone Protection configurations

in Panorama or directly on each appliance to confirm whether the portal is active and which source addresses are permitted to reach it. Any instance where the portal is accessible from untrusted zones or from the internet should be treated as critical priority.

For appliances where the portal is not required for business operations, Palo Alto Networks recommends disabling it entirely [1]. This eliminates the attack surface without requiring any network topology changes and is the strongest available mitigation for organizations that can tolerate it operationally. For appliances where the portal must remain active, access should be immediately restricted to only trusted internal IP address ranges using Security Policy rules or interface zone configurations that block untrusted source addresses from reaching the portal service. Implementing this restriction brings the effective CVSS score down from 9.3 to 8.7 and substantially reduces the exploitability of the vulnerability by removing it from internet-visible scanning surface [1].

Organizations running PAN-OS 11.1 or later should immediately verify that their Threat Prevention subscription is active and that the threat signature database has been updated to include the signature released on May 5, 2026 [1]. This signature provides active detection and blocking of exploit attempts against CVE-2026-0300 at the network layer, offering an additional defensive layer while patches are staged. Review firewall and system logs for any anomalous authentication portal activity, failed buffer-related errors, or unexpected outbound connections from the PAN-OS management plane that might indicate prior compromise. Palo Alto Networks' Unit 42 team should be consulted for current indicators of compromise associated with active exploitation campaigns.

Short-Term Mitigations

Organizations should establish tracking for the Palo Alto Networks patch release schedule and prioritize upgrading to the patched versions as they become available on each branch. The published remediation targets for each affected branch are: PAN-OS 10.2.18-h6, 10.2.16-h7, 10.2.13-h21, 10.2.10-h36, or 10.2.7-h34; PAN-OS 11.1.15, 11.1.13-h5, 11.1.10-h25, 11.1.7-h6, 11.1.6-h32, or 11.1.4-h33; PAN-OS 11.2.12, 11.2.10-h6, 11.2.7-h13, or 11.2.4-h17; and PAN-OS 12.1.7 or 12.1.4-h5 [1]. Given the rolling patch window through May 28, network-layer access controls should remain in place and not be relaxed on the assumption that a patch has been applied until the upgrade is confirmed and validated on each device.

Patch scheduling should account for the operational sensitivity of firewall appliances in production environments. Maintenance windows for perimeter firewalls require careful coordination with network operations and change management processes. Where possible, VM-Series appliances in virtualized environments may offer faster upgrade paths through snapshot-and-restore workflows, subject to Palo Alto Networks' upgrade guidance for virtualized deployments, allowing more rapid remediation

compared to physical PA-Series hardware. For organizations with large PAN-OS deployments, Panorama can be used to centrally identify unpatched appliances and coordinate upgrade scheduling across the fleet.

In parallel with patching, organizations should review their authentication portal configurations more broadly. The principle of least privilege applies to management and identity services as directly as it does to user access: network services that are exposed to untrusted networks—including firewalls, VPN endpoints, authentication portals, and management interfaces—represent an attack surface that should be systematically audited and minimized regardless of whether a specific CVE has been disclosed. This review is an appropriate trigger to identify any other PAN-OS services or management interfaces that may be unnecessarily exposed.

Strategic Considerations

CVE-2026-0300 reflects a broader pattern in enterprise network security: the authentication and identity services that sit at the edge of the network perimeter are themselves high-value targets. The User-ID Authentication Portal is a feature designed to map user identities to network traffic—an important capability for policy enforcement—but its location at the network boundary makes it an attractive attack surface when exposed to untrusted addresses. This vulnerability is not the first critical RCE discovered in PAN-OS boundary-facing services. CVE-2024-3400 exploited GlobalProtect [13] [14]; CVE-2025-0108 targeted the PAN-OS management web interface [15]; CVE-2026-0300 targets the Authentication Portal [1]. The pattern suggests that any internet-accessible PAN-OS service—regardless of its intended function—warrants ongoing scrutiny and hardened access controls.

Organizations should use this incident as an impetus to enforce network segmentation and access controls around all management and authentication interfaces on network security appliances, not just Authentication Portals. Management interfaces for firewalls, switches, and other network infrastructure should be accessible exclusively from dedicated, out-of-band management networks with strong authentication requirements. This architecture provides defense in depth independent of any specific vulnerability: even if a future critical RCE is discovered in a management service, restrictive network access controls limit the population of attacker positions from which the vulnerability can be reached.

As observed across recent network infrastructure CVEs, patches for critical vulnerabilities rarely arrive immediately. The seven-to-twenty-two day gap between the current date and the completion of Palo Alto Networks' patch rollout illustrates why compensating controls must be a durable part of vulnerability management strategy, not a temporary improvisation. The organizations best positioned to weather the pre-patch window are those that have invested in network segmentation, access restriction discipline, and security telemetry that can surface anomalous behavior on network infrastructure before a compromise escalates.

CSA Resource Alignment

This vulnerability and its remediation map directly to several CSA frameworks and guidance documents that provide the structural foundation for enterprise network security programs.

The CSA Cloud Controls Matrix (CCM)—extended and supplemented by the AI Controls Matrix (AICM), which adds AI-specific controls to the CCM baseline—addresses infrastructure vulnerability management under the Infrastructure & Virtualization Security (IVS) domain. IVS controls require organizations to maintain an inventory of network devices, apply security patches on a documented schedule, and enforce least-privilege access to management interfaces. The authentication portal exposure at the center of CVE-2026-0300 is precisely the condition these controls are designed to prevent: a service with elevated network privileges left accessible to untrusted sources due to misconfiguration or inattention to attack surface minimization.

CSA's Zero Trust guidance is directly applicable to the recommended mitigations. The zero trust model—verify explicitly, use least privilege access, assume breach—applies to network infrastructure services in the same way it applies to application access. The User-ID Authentication Portal, as a trust boundary service, should itself be subject to trust boundary controls: accessible only from authenticated, verified, and authorized network positions, not from arbitrary untrusted addresses. Organizations that have implemented zero trust network architecture (ZTNA) as a user access model but have not applied equivalent controls to the management and identity infrastructure itself should treat this gap as a priority.

The STAR (Security Trust Assurance and Risk) program provides a continuous assurance framework that is relevant to cloud and hybrid network security monitoring. Organizations using managed security service providers or cloud-based security operations centers should verify that their monitoring coverage extends to PAN-OS management plane telemetry, not only to traffic passing through the firewall. Detection of post-exploitation activity on a compromised PAN-OS appliance requires visibility into the device's own system logs, configuration change events, and outbound connections—telemetry that is distinct from the traffic inspection data the firewall generates for network monitoring purposes.

CSA's ongoing work in the Trusted Cloud Initiative (TCI) and shared responsibility frameworks is also relevant for organizations using VM-Series firewalls in public cloud environments. In infrastructure-as-a-service deployments, the cloud provider manages the physical hardware and hypervisor layer, but the VM-Series PAN-OS instance and its configuration are customer responsibilities. The shared responsibility boundary does not extend to automated OS patching for customer-managed virtual appliances; organizations operating VM-Series firewalls in AWS, Azure, or GCP are fully responsible for their own patch management and access restriction configuration for these instances.

References

[1] Palo Alto Networks. "CVE-2026-0300 PAN-OS: Unauthenticated User Initiated Buffer Overflow Vulnerability in User-ID™ Authentication Portal." Palo Alto Networks Security Advisories, May 2026.

[2] Help Net Security. "Root-level RCE vulnerability in Palo Alto firewalls exploited (CVE-2026-0300)." Help Net Security, May 6, 2026.

[3] Security Online. "Exploited in the Wild: Critical PAN-OS Buffer Overflow Grants Root Access to Palo Alto Firewalls." Security Online, May 2026.

[4] The Hacker News. "Palo Alto PAN-OS Flaw Under Active Exploitation Enables Remote Code Execution." The Hacker News, May 2026.

[5] SOCRadar. "CVE-2026-0300 Enables Root RCE in PAN-OS Captive Portal." SOCRadar, May 2026.

[6] Bleeping Computer. "Palo Alto Networks warns of firewall RCE zero-day exploited in attacks." Bleeping Computer, May 2026.

[7] SecurityWeek. "Palo Alto Networks to Patch Zero-Day Exploited to Hack Firewalls." SecurityWeek, May 2026.

[8] GBHackers. "Critical Palo Alto Firewall Vulnerability Enables Attackers to Gain Root Privileges." GBHackers, May 2026.

[9] Tenable. "CVE-2026-0300." Tenable Vulnerability Database, May 2026.

[10] Cyber Security Agency of Singapore. "Active Exploitation of Palo Alto Networks PAN-OS Software." CSA Singapore Alert AL-2026-048, May 2026.

[11] IONIX. "CVE-2026-0300 - Palo Alto Networks PAN-OS Captive Portal Unauthenticated RCE (Actively Exploited)." IONIX Threat Center, May 2026.

[12] Security Affairs. "Palo Alto Networks PAN-OS flaw exploited for remote code execution." Security Affairs, May 2026.

[13] Volexity. "Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in Global Protect (CVE-2024-3400)." Volexity Threat Research, April 12, 2024.

© 2026 Cloud Security Alliance. AI-assisted Rapid Research.

[14] Palo Alto Networks. "CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway." Palo Alto Networks Security Advisories, April 2024.

[15] Palo Alto Networks. "CVE-2025-0108 PAN-OS: Authentication Bypass in the Management Web Interface." Palo Alto Networks Security Advisories, February 2025.