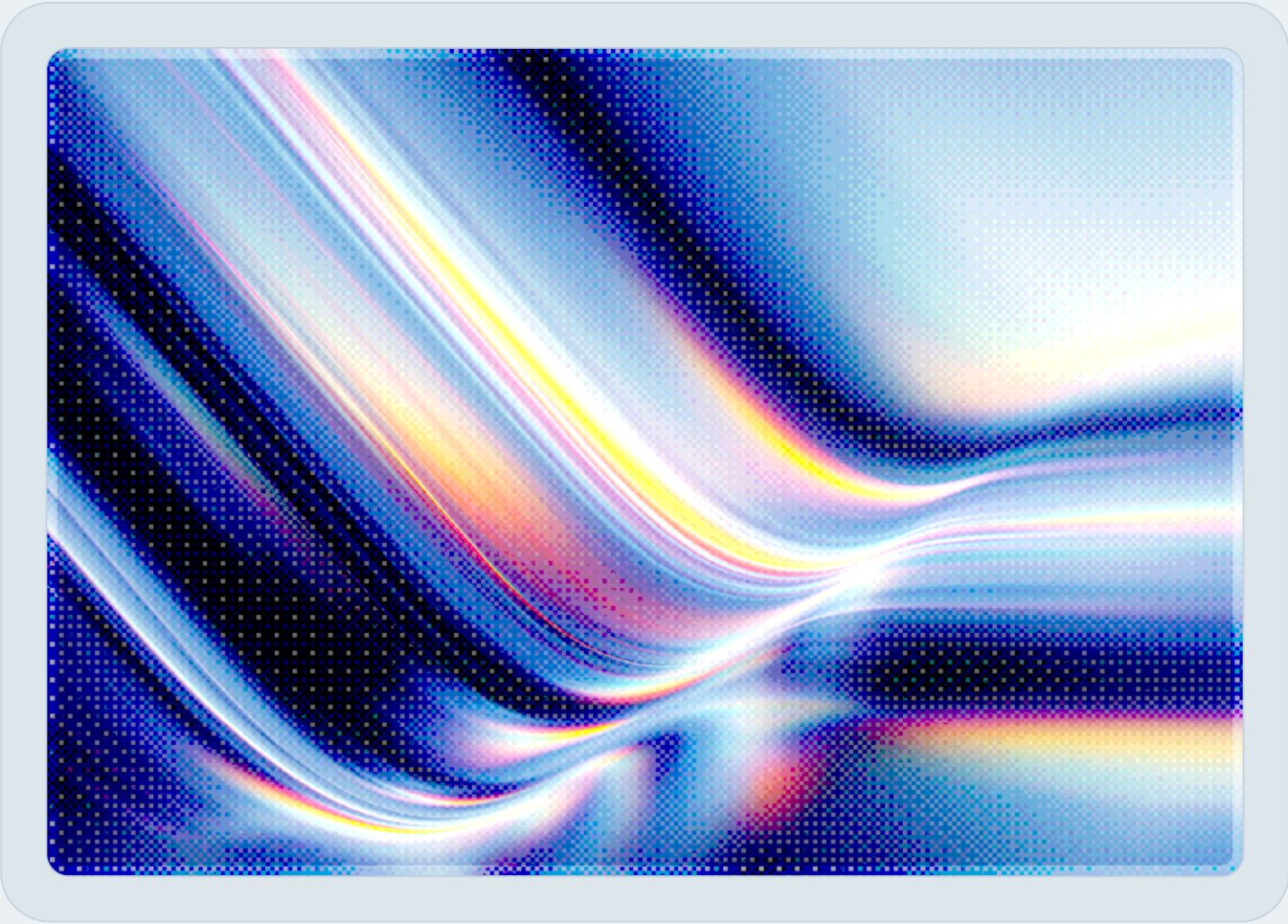
CSAI Foundation | Cloud Security Alliance

CVE-2026-0300: Root-Level RCE in PAN-OS Under Active Exploitation

2026-05-08

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

CVE-2026-0300 is a critical-severity buffer overflow vulnerability in the Palo Alto Networks PAN-OS User-ID™ Authentication Portal, carrying a CVSS score of 9.3 when the portal is accessible from untrusted networks [1]. An unauthenticated remote attacker can send specially crafted packets to the portal to execute arbitrary code with root privileges on affected PA-Series and VM-Series firewalls.

Active exploitation was first detected on April 9, 2026, with confirmed successful code execution achieved approximately one week later [2]. Unit 42 is actively tracking a threat cluster, designated CL-STA-1132, that is assessed with high confidence to be state-sponsored and has used this vulnerability to gain persistent root-level access to victim firewalls, conduct log tampering, and enumerate Active Directory environments using the firewall's own service account credentials [3].

CISA added CVE-2026-0300 to the Known Exploited Vulnerabilities (KEV) catalog on May 6, 2026, with a remediation deadline of May 27, 2026, for Federal Civilian Executive Branch agencies [4]. Palo Alto Networks has confirmed that patches across the affected PAN-OS version branches will begin rolling out on approximately May 13, 2026, with the full patching cycle completing around May 28, 2026 [1]. Until patches are available and deployed, organizations should treat this as a zero-day and prioritize immediate protective action.

Background

Palo Alto Networks PA-Series and VM-Series firewalls are widely deployed across enterprise, government, and critical infrastructure environments, where they typically serve as the primary enforcement point for traffic inspection, segmentation, and policy enforcement. PAN-OS is the operating system underpinning these devices, and its security is foundational to the security posture of any organization that relies on it. Compromise of a PAN-OS device effectively grants an adversary a position of privilege within the network — one that is trusted by downstream systems, often has access to routing tables and policy configurations, and where security teams may apply less scrutiny to monitoring and patching than to endpoint environments, in part because network devices are often treated as infrastructure rather than managed endpoints.

The specific component affected by CVE-2026-0300 is the User-ID™ Authentication Portal, commonly referred to as the Captive Portal. This feature enables organizations to authenticate users before granting them network access, and it communicates over ports 6081 and 6082. When enabled and exposed to untrusted networks — including the public internet — the portal presents an attack surface that, in this case, can be exploited without any authentication [5]. The portal is not enabled by default in all configurations, but it is a commonly deployed feature in environments that use identity-based policy enforcement.

The vulnerability itself is classified under CWE-787 (Out-of-Bounds Write), the same class of memory corruption that underlies many of the most severe network device compromises over the past decade. An out-of-bounds write in a network-facing service running with elevated privilege is one of the most dangerous conditions in embedded operating systems: in most configurations, application-layer mitigations alone cannot reliably prevent exploitation of memory corruption at this level, and hardware and OS-layer protections such as ASLR or stack canaries may raise the bar but do not eliminate the risk [6]. The resulting code execution inherits the service's runtime context — in this case, root. Palo Alto Networks has confirmed that Prisma Access, Cloud NGFW, and Panorama appliances are not affected [1].

Security Analysis

Vulnerability Mechanics and Attack Surface

The root-cause classification of CWE-787 indicates that the vulnerability arises from a failure to properly validate the length or content of attacker-controlled input before writing it to a fixed-size buffer. When a specially crafted packet arrives at the User-ID Authentication Portal service, it overwrites adjacent memory regions, allowing an attacker to redirect code execution. Because the affected service runs with root privileges, the resulting execution context is unrestricted — the attacker gains the highest privilege level available on the operating system without supplying any credentials [5][6].

The attack requires only network-level access to the portal. No credentials, session tokens, or prior foothold are necessary. This is particularly significant because the portal is specifically designed to be accessible to unauthenticated users (it is an authentication portal by function), meaning that organizations may have intentionally exposed it to broad network segments or the internet. The CVSS score of 9.3 reflects this pre-authentication reachability; the score drops to 8.7 when portal access is restricted to trusted internal IP addresses — a High severity designation under CVSS v4.0 that still warrants urgent treatment [1].

Observed Exploitation Timeline and Attack Chain

The exploitation timeline published by Unit 42 provides an unusually detailed picture of how the vulnerability was weaponized in practice [3]. Initial attempts to trigger the vulnerability were logged as early as April 9, 2026, but these early probes were unsuccessful, suggesting that the attacker was actively developing or refining their exploit against a live target. Approximately one week later — around April 16 — successful remote code execution was achieved, and shellcode was injected into the running process.

The initial exploitation was followed by deliberate operational security measures. The attacker performed log cleanup on the compromised device before deploying additional tooling roughly four days after the initial compromise. This post-exploitation phase involved Active Directory enumeration conducted using the firewall's own service account credentials, a technique that enables reconnaissance of the internal directory environment while appearing to originate from a trusted, internal network device. This pattern of behavior — leveraging the firewall's trusted identity against downstream systems — is consistent with nation-state tradecraft focused on durable access and lateral movement rather than immediately destructive action [3].

The time between first observed probe (April 9) and CISA's KEV listing (May 6) represents nearly a month during which the vulnerability was actively exploited in the wild without a vendor patch available. This gap underscores the severity of the exposure for organizations that cannot immediately disable or restrict the affected functionality.

Threat Actor Assessment

Unit 42 has designated the observed activity cluster as CL-STA-1132 and assesses it as likely state-sponsored [3]. This assessment is based on the sophistication of the exploit development (successful RCE against a hardened network operating system within approximately one week of initial probing), the deliberate operational security posture (log sanitization prior to tool deployment), and the post-compromise focus on intelligence gathering rather than ransomware or other financially motivated activity. The specific sponsoring nation-state has not been publicly attributed at the time of this writing.

State-sponsored threat actors have historically demonstrated a strong interest in network infrastructure appliances as initial access vectors precisely because they sit at the boundary of enterprise environments, have broad network visibility, often hold valuable credentials, and are less likely to receive the same endpoint detection coverage as user workstations. The combination of unauthenticated root RCE on a device trusted by the internal network makes CVE-2026-0300 a particularly valuable tool for espionage campaigns.

Scope of Exposure

PA-Series physical firewalls and VM-Series virtual appliances are deployed across enterprise, government, and critical infrastructure environments; the full scope of vulnerable exposures depends on each organization's portal configuration. The degree of exposure depends on whether the User-ID Authentication Portal is enabled and, if so, whether it is accessible from untrusted networks or the public internet. Organizations that have restricted portal access to trusted internal IP ranges face a materially lower — though still elevated — risk. Organizations with the portal exposed to the internet face the highest urgency for action [1].

Virtual machine-based firewall deployments in cloud environments introduce an additional dimension of exposure: VM-Series instances running in public cloud environments may have the portal inadvertently reachable from internet-facing subnets depending on security group and routing configurations. Cloud-deployed firewalls warrant specific examination of their network accessibility.

Recommendations

Immediate Actions

The absence of a vendor patch until approximately May 13, 2026, makes immediate protective configuration changes essential for all affected organizations. Palo Alto Networks' primary recommended mitigation is to restrict access to the User-ID Authentication Portal to trusted IP addresses only, or to disable the portal entirely if it is not required for operational purposes [1]. Organizations should audit their firewall configurations immediately to determine whether the portal is enabled and, if so, what network ranges can reach it.

For Federal Civilian Executive Branch agencies, CISA's May 27, 2026, deadline under the KEV catalog directive is binding [4]. Agencies running PAN-OS versions whose patches are not released until the May 28 tranche — after the CISA deadline — must implement the configuration-based workaround to demonstrate compliance by May 27, then apply the vendor patch upon release.

A network-layer firewall rule or access control list (ACL) restricting inbound connections to ports 6081 and 6082 to explicitly enumerated trusted IP ranges provides an alternative control layer for organizations that may not be able to modify the PAN-OS configuration directly. However, this approach should be treated as a defense-in-depth measure and not a substitute for applying the configuration change within PAN-OS itself.

Short-Term Mitigations

After implementing the immediate configuration change, organizations should enhance monitoring for indicators consistent with the observed attack chain. Network traffic logs should be reviewed for anomalous connection patterns targeting ports 6081 and 6082 originating from unexpected source IP addresses, particularly across time periods coinciding with the April 9 to May 6 window. Log integrity on PAN-OS devices should be verified, as the observed attacker performed log cleanup post-compromise; gaps or anomalies in system and event logs on firewall devices may indicate prior compromise.

Once patches become available in the May 13–28 window, organizations should treat PAN-OS patching for this CVE as emergency remediation, following change management procedures proportionate to the severity. The staggered patch availability across PAN-OS version branches means that teams should confirm the specific version branch in use and monitor Palo Alto Networks' security advisory [1] for the corresponding release date. Organizations running versions that receive patches in the May 28 tranche should not defer action until that date — they should maintain the configuration-based workaround until the patch is applied.

Third-party managed security service providers and network operations teams should verify that any PA-Series or VM-Series firewalls managed on behalf of clients have been assessed. Supply chain and managed service exposure represents a secondary propagation vector: a compromised upstream provider's firewall may extend adversary access into multiple downstream client networks.

Strategic Considerations

CVE-2026-0300 is a reminder that network security appliances are not immune to the classes of vulnerability that affect general-purpose operating systems. Organizations that treat firewalls as inherently trusted components — and that therefore apply less rigorous patching cadence, less monitoring, or less segmentation to their firewall management interfaces — should reassess that posture. The firewall's privileged network position makes it a high-value target precisely because of the access it provides once compromised.

Zero Trust architecture principles apply directly to this scenario. In a Zero Trust model, no device — including a firewall — is assumed to be trustworthy by virtue of its position on the network. The firewall's service account should have the minimum permissions necessary for its functions; if AD enumeration via a firewall service account is possible, that service account's permissions should be reviewed. Network access to management interfaces and authenticated services like the User-ID Portal should be constrained to named, verified sources. The assumption that network infrastructure appliances are inherently trustworthy is precisely the assumption this class of attack exploits.

Organizations should also consider whether their current vendor risk and patch management processes are calibrated to respond to zero-day exploitation scenarios with sufficient speed. The period between initial exploitation (April 9) and the first vendor patch (estimated May 13) is 34 days — a window during which configuration-based controls — access restriction and portal disablement — represent the primary and most direct defensive measures. A security program oriented primarily toward patch-based remediation, without the operational capacity to rapidly implement configuration workarounds, will be exposed for that entire interval.

CSA Resource Alignment

Several CSA frameworks and publications directly inform the organizational response to CVE-2026-0300 and the broader category of network infrastructure zero-day vulnerabilities.

The CSA Cloud Controls Matrix (CCM) v4.1 addresses this scenario through multiple control domains [7]. The Threat and Vulnerability Management (TVM) domain specifies requirements for identifying, assessing, and prioritizing the remediation of vulnerabilities on network devices, including the expectation that critical and high-severity vulnerabilities receive expedited treatment. The Infrastructure and Virtualization Security (IVS) domain addresses configuration management for network infrastructure, including the principle that administrative access to network devices should be restricted to trusted, enumerated sources — a control that, if implemented, would have limited the exploitability of CVE-2026-0300 in many environments. The Logging and Monitoring (LOG) domain requirements for audit log retention and integrity are also directly relevant given the observed attacker behavior of log tampering post-compromise.

CSA's Zero Trust guidance [8] provides a strategic framework that is directly applicable to the post-compromise activity pattern observed with CL-STA-1132. The attacker's use of the firewall's service account credentials to enumerate Active Directory illustrates the risk of implicit trust in network infrastructure identities. A Zero Trust architecture would apply least-privilege principles to the firewall's service account, would require explicit verification of any access request originating from infrastructure devices, and would segment the blast radius of a compromised network appliance from the broader directory environment.

The CSA Security Trust Assurance and Risk (STAR) registry provides a mechanism for organizations to assess the security posture of cloud and infrastructure vendors [9]. Organizations that rely on managed firewall services or cloud-delivered network security should use the STAR program to evaluate their providers' vulnerability response practices, including time-to-patch commitments for critical CVEs and the operational security of shared management infrastructure.

For organizations using VM-Series firewalls in cloud environments, the shared responsibility model demands particular attention. The cloud provider is responsible for the underlying compute infrastructure, but the customer is responsible for the operating system and application layer — including PAN-OS configuration and patching — on customer-managed VM-Series instances. This responsibility boundary must be clearly understood and operationalized, as CISA KEV compliance obligations and internal security standards apply to these cloud-deployed instances just as they do to on-premises hardware.

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] BleepingComputer. "Palo Alto Networks firewall zero-day exploited for nearly a month." BleepingComputer, May 2026.

[3] Palo Alto Networks Unit 42. "Threat Brief: Exploitation of PAN-OS Captive Portal Zero-Day for Unauthenticated Remote Code Execution." Unit 42, May 2026.

[4] CISA. "CISA Adds One Known Exploited Vulnerability to Catalog." Cybersecurity and Infrastructure Security Agency, May 6, 2026.

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

[6] Rapid7. "Critical Buffer Overflow in Palo Alto Networks PAN-OS User-ID Authentication Portal (CVE-2026-0300)." Rapid7 Emergent Threat Response, May 2026.

[7] Cloud Security Alliance. "Cloud Controls Matrix v4.1." CSA, 2025.

[8] Cloud Security Alliance. "Zero Trust Advancement Center." CSA, 2024.

[9] Cloud Security Alliance. "STAR: Security Trust Assurance and Risk." CSA, 2024.

Further Reading

- SecurityWeek. "Palo Alto Networks to Patch Zero-Day Exploited to Hack Firewalls." SecurityWeek, May 2026.
- Wiz. "Critical Buffer Overflow Vulnerability in PAN-OS Exploited in-the-Wild." Wiz Blog, May 2026.