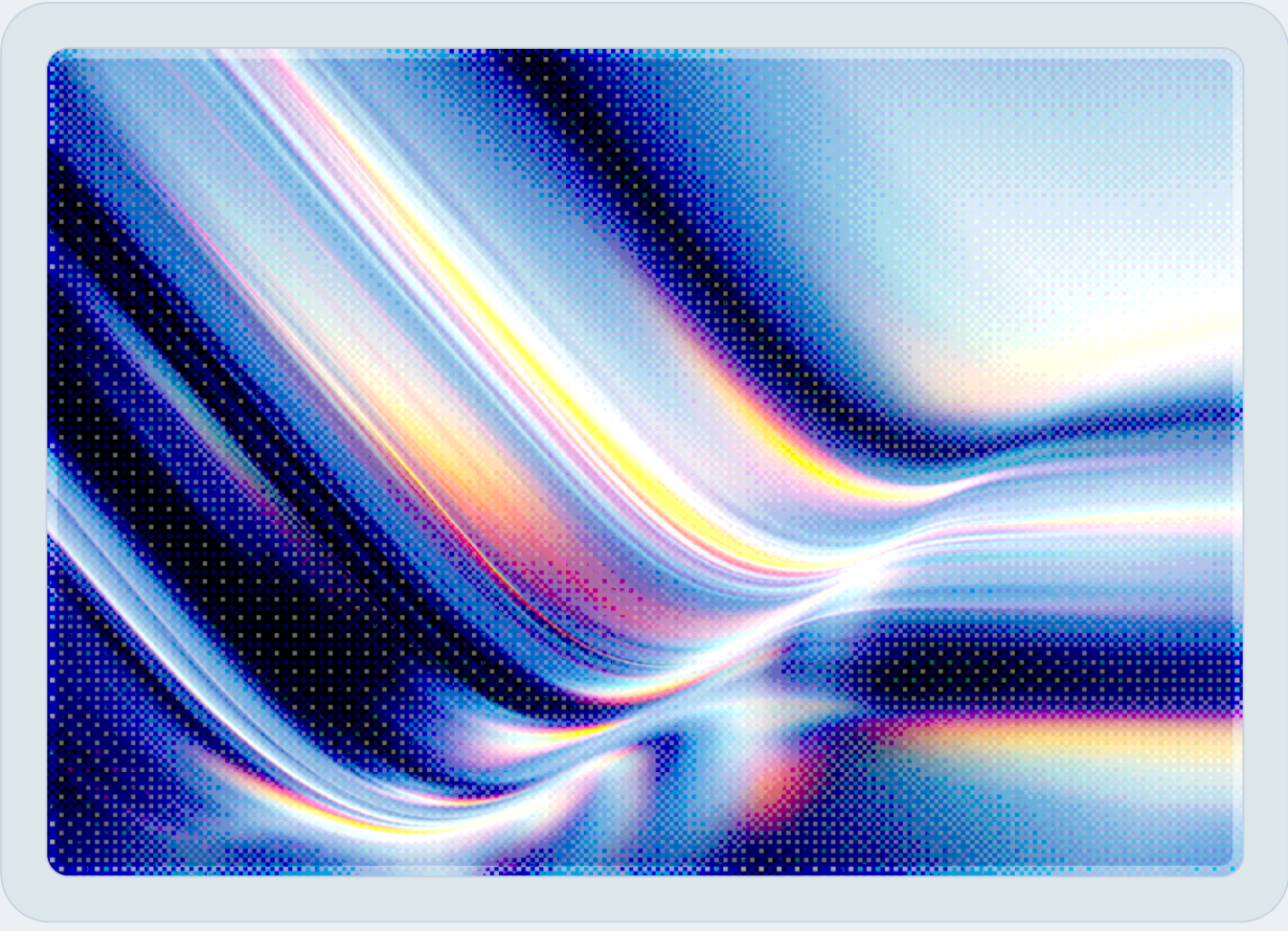
CSAI Foundation | Cloud Security Alliance

PAN-OS GlobalProtect Auth Bypass: Active NGFW Exploitation

CVE-2026-0257 Enables Unauthorized VPN Access Across Affected Palo Alto Deployments

2026-06-10

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

A cookie-forging vulnerability in Palo Alto Networks' GlobalProtect VPN component is enabling unauthenticated attackers to establish fully authorized tunnel sessions into enterprise networks, bypassing the perimeter firewall that organizations depend on as a foundational trust boundary. CISA added CVE-2026-0257 to its Known Exploited Vulnerabilities catalog on May 29, 2026, ordering Federal Civilian Executive Branch agencies to remediate by June 1, 2026 [1][14].

- CVE-2026-0257 (CVSS 3.1: 9.1; Palo Alto CVSS 4.0: 7.8) allows a remote unauthenticated attacker to forge a valid authentication override cookie and establish an unauthorized VPN session through GlobalProtect portal or gateway components [2][3].
- The root cause is a certificate reuse flaw: when an organization uses the same TLS certificate for the HTTPS service and the cookie signing function, an attacker can extract the public key from the server's TLS handshake and use it to craft a cryptographically valid cookie — requiring no stolen credentials [4][5].
- Rapid7 MDR observed confirmed exploitation beginning May 17, 2026, followed by a second distinct wave on May 21, 2026, with both waves assessed as likely originating from a single threat actor based on consistent device identifiers [4].
- Attackers authenticated as local administrator accounts via forged cookies, then were assigned internal VPN IP addresses — gaining routed access to corporate networks as if they were legitimate VPN users [4][6].
- Patches are available for all affected PAN-OS versions (10.2, 11.1, 11.2, 12.1) and Prisma Access (10.2, 11.2). Where immediate patching is not possible, organizations can mitigate by generating a dedicated certificate used exclusively for authentication override cookies [2].

Background

Palo Alto Networks' GlobalProtect is one of the most widely deployed enterprise VPN and remote access solutions, integrated into the company's next-generation firewall (NGFW) platform, PAN-OS. GlobalProtect serves as both the endpoint agent that connects remote workers and a gateway that

enforces zero-trust network access policies before permitting traffic to internal resources. Compromise of a GlobalProtect gateway is therefore qualitatively different from compromising an application server: it undermines the network-layer security boundary that all downstream controls depend on.

PAN-OS firewalls have attracted sustained adversarial attention throughout 2025 and 2026 due to their privileged network position and the breadth of their enterprise deployment. CVE-2026-0257 is the latest in a series of high-severity vulnerabilities affecting the platform, coinciding with the ongoing exploitation of CVE-2026-0300, a buffer overflow in the PAN-OS Captive Portal service that carries a CVSS 3.1 score of 9.3 [7][8][16] and has been linked by Unit 42 to likely state-sponsored threat activity tracked as cluster CL-STA-1132 [7][8]. The two vulnerabilities are distinct but share the same target platform, and their concurrent active exploitation has elevated the urgency of remediating any unpatched PAN-OS deployment.

Palo Alto Networks published its initial advisory for CVE-2026-0257 on May 13, 2026, with a severity rating that was subsequently revised upward to 7.8 under CVSS 4.0 and 9.1 under CVSS 3.1 as the full impact of active exploitation became clear and the exploitability characteristics were better understood [2][3]. The gap between initial disclosure and confirmed exploitation in the wild was approximately four days — a window that leaves little margin for organizations to assess, prioritize, and deploy patches before active attacks begin [4].

Security Analysis

The Cookie Trust Failure

GlobalProtect's authentication override feature is a convenience mechanism that allows users who have completed multi-factor authentication to receive a signed cookie from the portal. On subsequent connections — to the same portal or to a configured gateway — GlobalProtect can present this cookie instead of re-authenticating the user from scratch. The design reduces authentication friction, particularly for mobile users roaming between gateways, but it creates a trust dependency: the gateway must accept the cookie as proof that the portal already validated the user's identity.

CVE-2026-0257 arises from an implementation flaw in how that cookie trust is established. According to Palo Alto Networks' advisory and Rapid7's technical analysis, the vulnerability exists when GlobalProtect is configured to use authentication override cookies and the certificate used to encrypt those cookies is the same certificate that serves the HTTPS interface of the portal or gateway [2][4].

Under this configuration — common enough that Palo Alto Networks documented it explicitly as the vulnerable case — the public key needed to encrypt a cookie that the server will accept is freely available to any external party who connects to the service and inspects its TLS certificate [5].

Because the server does not perform cryptographic signature verification on the cookie content — it decrypts the cookie and trusts what it finds — an attacker who obtains the public key can construct a cookie containing arbitrary claims about the user's identity and authentication state [5]. Rapid7 released a proof-of-concept tool (`forge_cookie.py`) that automates this process: connecting to the target's GlobalProtect portal to retrieve its TLS certificate, extracting the public key, generating a cookie claiming a valid authenticated session for a specified username, and submitting that cookie to the gateway [4]. Two public PoC repositories also appeared on GitHub shortly after the Rapid7 disclosure, lowering the skill threshold for exploitation across the broader attacker community [9][10].

Observed Exploitation Activity

Rapid7's Managed Detection and Response team first observed exploitation on May 17, 2026, in a customer environment where forged authentication override cookies were submitted to GlobalProtect gateways targeting the local administrator account [4]. The attack pattern — impersonating the local admin rather than attempting to spoof a specific end-user — suggests the threat actor may have been probing for configurations where the local administrator account is permitted to authenticate through GlobalProtect, an approach that maximizes success probability across diverse target environments.

A second exploitation wave occurred on May 21, 2026, affecting multiple Rapid7 customer environments in close succession. In the second wave, the sequence extended beyond initial authentication: following the cookie submission and VPN IP assignment, the attacker's session was observed with routed access to internal network ranges [4][6]. Because both waves exhibited a consistent MAC address in the VPN session metadata, Rapid7 assesses that both campaigns are attributable to the same threat actor or coordinated operation [4]. Attack infrastructure in both waves was hosted on commercial cloud providers — Vultr and Dromatics Systems — consistent with operationally fast, cost-conscious threat actors who use disposable infrastructure to complicate attribution [4][6][15].

No confirmed post-exploitation lateral movement, data exfiltration, or persistence mechanisms have been documented in public incident disclosures as of this writing. However, a successfully established VPN session through GlobalProtect grants the attacker routed IP-layer access to internal network segments with the same privileges as the impersonated account — which, in cases where the local administrator account was targeted, may be substantial. The absence of confirmed follow-on activity in public reporting does not imply the sessions were used only for reconnaissance; it reflects the limits of what defenders have disclosed at this stage of investigation.

Scope and Scale of Exposure

Affected PAN-OS versions span a wide release window: 10.2, 11.1, 11.2, and 12.1, as well as Prisma Access versions 10.2 and 11.2 [2]. Crucially, a device is vulnerable only when three conditions are simultaneously true: GlobalProtect portal or gateway is configured, the authentication override cookie feature is enabled, and the same certificate is used for both the HTTPS service and the override cookie function [2]. In environments that use a dedicated, separately-issued certificate for cookie signing — as Palo Alto Networks now strongly recommends — the vulnerability is not present regardless of PAN-OS version.

Estimates of internet-exposed PAN-OS deployments vary, but research by Wiz in May 2026 found that approximately 7% of environments scanned had publicly reachable PAN-OS instances [12]. Shodan data around the same period showed 67 hosts responding on port 6081, the default GlobalProtect portal port [12]. These figures likely represent a conservative lower bound of the actual attack surface, as many GlobalProtect portals use standard HTTPS port 443, which is not easily distinguished from other HTTPS services in passive scan data. Sector-level analysis found concentrated exposure among industrial organizations, telecommunications providers, and energy sector entities, pointing to a risk profile that extends well beyond general enterprise IT [13].

Palo Alto Networks commands one of the largest enterprise NGFW deployments globally, meaning even a modest percentage of vulnerable configurations translates to a substantial population of exposed organizations. The scale of affected PAN-OS versions — spanning more than two years of releases across both on-premises and cloud-hosted deployments — means organizations cannot assume they are out of scope without an explicit configuration review.

Relationship to Broader NGFW Exploitation Trends

CVE-2026-0257 fits a documented pattern of adversaries targeting network security appliances as initial access vectors. Edge devices — firewalls, VPN concentrators, and remote access gateways — occupy a structurally attractive position for attackers: they are internet-facing by design, they operate with elevated network privileges, and they often have more limited EDR visibility than internal servers, as the sensors available for traditional host-based detection do not apply to purpose-built network appliances. The concurrent exploitation of CVE-2026-0300, affecting a different PAN-OS component (the Captive Portal service), suggests threat actors are performing broad reconnaissance against PAN-OS infrastructure rather than targeting individual vulnerabilities opportunistically [7][8]. This dual-vector activity reinforces the assessment that unpatched PAN-OS deployments face active, sustained adversarial attention across multiple vulnerability classes.

Recommendations

Immediate Actions

Organizations running affected PAN-OS versions should treat this as a priority incident requiring action within 24–72 hours rather than within a normal patch cycle. Any PAN-OS deployment running versions 10.2, 11.1, 11.2, or 12.1, or Prisma Access 10.2 or 11.2, with GlobalProtect configured should be assessed immediately.

The definitive remediation is patching to a fixed PAN-OS release. Palo Alto Networks has published updated software for all affected branches — PAN-OS 12.1, 11.2, 11.1, and 10.2 — and for Prisma Access 11.2.0 and 10.2.0 [2]. Organizations should consult the official Palo Alto Networks security advisory for the minimum fixed version within each branch and apply the update as soon as operational conditions allow.

Where patching cannot be completed immediately, Palo Alto Networks has documented two configuration-based mitigations [2]. The first option is to disable the authentication override cookie feature entirely; this eliminates the attack surface but requires end users to complete full authentication on each VPN session. The second option is to generate a new certificate used exclusively for authentication override cookie signing, ensuring this certificate is not exposed through the HTTPS interface; this preserves the convenience feature while closing the cryptographic exposure. Both mitigations should be considered temporary bridges to patching rather than permanent configurations, as the authentication override feature serves a legitimate operational purpose.

Short-Term Mitigations

Security teams should review GlobalProtect logs for anomalous authentication override cookie submissions, particularly those targeting the local administrator account or originating from unexpected geographic locations or IP ranges. Authentication events from infrastructure hosted on Vultr and Dromatics Systems — the providers documented in the May exploitation waves [4][6] — warrant heightened scrutiny. Defenders may also wish to apply elevated alert thresholds to other commercial cloud hosting providers that offer rapid, low-cost compute with minimal identity verification requirements. Indicators of compromise from Rapid7's incident observations should be ingested into SIEM and network detection tools [4][11].

Organizations should also verify that GlobalProtect is not configured to permit the local administrator account to authenticate through the portal. Restricting VPN authentication to domain accounts with active directory controls reduces the value of forged cookies that impersonate local credentials.

Network segmentation controls should be reviewed to ensure that VPN-assigned IP addresses are placed in appropriately scoped network ranges. A GlobalProtect user granted a VPN IP should not, by default, have flat routed access to all internal segments; zero-trust network access policies enforced by the firewall itself should restrict lateral reach to resources explicitly authorized for that user role. Where Panorama is deployed, the management console should be confirmed as not internet-exposed; Palo Alto Networks has confirmed that Panorama itself is not affected by CVE-2026-0257 [2], but Panorama exposure creates a separate high-value attack surface.

Strategic Considerations

The CVE-2026-0257 incident illustrates a recurring structural tension in enterprise security architecture: the operational convenience features that reduce friction for end users and administrators frequently introduce cryptographic shortcuts that expand attack surface. Authentication override mechanisms, delegated trust tokens, and persistent session cookies are all legitimate engineering patterns, but each creates a dependency on the integrity of the underlying signing or encryption material. When that material is shared across functions with different trust boundaries — as in this case, where the same certificate served both TLS and cookie signing — an attacker needs only one of those exposure paths to compromise the others.

The appropriate architectural response is to enforce strict certificate segregation as a standing policy: certificates used for session token signing or authentication delegation should be explicitly prohibited from serving as the TLS identity of any internet-facing interface. This principle extends beyond GlobalProtect to any system that issues bearer tokens using public-key cryptography, including internal certificate authorities, token-signing services, and enterprise authentication platforms. Enforcing this through configuration management tooling — rather than relying on operator discipline at deployment time — provides durable protection against the class of vulnerability CVE-2026-0257 represents.

CSA Resource Alignment

This vulnerability and its exploitation pattern map to several existing CSA frameworks that organizations can use to structure their response and strengthen long-term posture.

The CSA **Zero Trust Guidance** provides the architectural framework most directly applicable to the failures that CVE-2026-0257 exploits. Zero trust principles require that network access be continuously verified against identity and device posture rather than granted based on network location or a one-time

authentication artifact. A GlobalProtect deployment relying on long-lived authentication override cookies without per-session posture reassessment deviates from zero trust intent; the remediation and mitigation steps above should be evaluated against an organization's zero trust maturity roadmap.

The CSA **AI Controls Matrix (AICM)**, which extends the Cloud Controls Matrix (CCM) into AI-augmented and cloud-native environments, provides relevant controls in the Identity and Access Management (IAM) domain, particularly IAM-02 (Credential Lifecycle and Provisioning Management) and IAM-06 (User Access Provisioning), which require that credentials — including session tokens and authentication cookies — be managed with appropriate expiry, revocation, and segregation controls. The certificate reuse at the core of CVE-2026-0257 represents a failure of credential segmentation that these controls are designed to prevent.

The **MAESTRO** (Multilayer AI Security Threat and Risk Observatory) framework, while developed in the context of agentic AI threat modeling, captures a threat class directly relevant here: trust delegation abuse. MAESTRO Layer 5 (Secure Channels and Communication) addresses the integrity requirements for inter-component authentication tokens in automated systems. The principle — that signing material for trust tokens must be isolated from presentation-layer certificates — applies equally in traditional NGFW contexts as in AI pipeline architectures. Security teams building AI-assisted network operations or using AI agents to manage firewall configuration should ensure the same certificate segregation principles are enforced in those contexts.

Finally, CSA's **STAR (Security Trust Assurance and Risk)** registry provides a mechanism for organizations to assess vendor security posture, including how vendors disclose and remediate vulnerabilities in their products. The evolving severity rating of CVE-2026-0257 — revised upward from its initial publication upon fuller understanding of its exploitability — highlights the importance of continuous monitoring of vendor advisories after initial publication, rather than treating the first-day rating as final. Organizations should incorporate vendor advisory revision tracking into their vulnerability management programs.

References

[1] CISA. "CISA Adds One Known Exploited Vulnerability to Catalog." CISA, May 29, 2026.

[2] Palo Alto Networks. "CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities." Palo Alto Networks Security Advisories, May 2026.

[3] NIST National Vulnerability Database. "CVE-2026-0257 Detail." NVD, May 2026.

[4] Rapid7. "Rapid7 Observed Exploitation of PAN-OS GlobalProtect Authentication Bypass Vulnerability (CVE-2026-0257)." Rapid7 Blog, May 2026.

[5] Penligent. "CVE-2026-0257, The GlobalProtect Auth Bypass That Turns Cookies Into VPN Access." Penligent Security Labs, May 2026.

[6] The Hacker News. "PAN-OS GlobalProtect Authentication Bypass (CVE-2026-0257) Under Active Exploitation." The Hacker News, May 2026.

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

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

[9] sfewer-r7 (Rapid7). "CVE-2026-0257: Proof-of-concept script to leverage the PAN-OS GlobalProtect authentication bypass." GitHub, May 2026.

[10] bolubey. "CVE-2026-0257: PAN-OS GlobalProtect Authentication Bypass." GitHub, May 2026.

[11] Help Net Security. "Hackers are exploiting Palo Alto GlobalProtect VPN authentication bypass (CVE-2026-0257)." Help Net Security, June 2026.

[12] Unit 42 / Palo Alto Networks. "Threat Brief: Active Exploitation of PAN-OS CVE-2026-0257." Unit 42, June 2026.

[13] CyCognito. "Emerging Threat: CVE-2026-0257 – PAN-OS GlobalProtect Authentication Bypass via Forged Override Cookies." CyCognito Blog, May 2026.

[14] Security Affairs. "U.S. CISA adds Palo Alto Networks PAN-OS flaw to its Known Exploited Vulnerabilities catalog." Security Affairs, May 2026.

[15] CyberScoop. "Attackers are exploiting Palo Alto Networks defect that initially flew under the radar." CyberScoop, June 2026.

[16] NIST National Vulnerability Database. "CVE-2026-0300 Detail." NVD, 2026.