Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-0257 Fuels GlobalProtect Authentication Bypass Attacks

Date of Publication	Admiralty Code	TA Number
June 02, 2026	A1	TA2026149

Summary

First Seen: May 13, 2026
Affected Products: Palo Alto Networks PAN-OS 10.2, 11.1, 11.2, 12.1; Prisma Access 10.2, 11.2
Impact: Palo Alto Networks has warned that attackers are actively exploiting CVE-2026-0257, a critical authentication bypass flaw affecting PAN-OS and Prisma Access deployments using GlobalProtect authentication override cookies. The vulnerability allows threat actors to forge trusted authentication cookies and gain unauthorized access without valid credentials, potentially opening a path into internal networks. With exploitation already observed across multiple organizations, the flaw highlights how a seemingly convenient authentication feature can become a serious security risk when misconfigured, making immediate patching and configuration reviews essential for exposed environments.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-0257	Palo Alto Networks PAN-OS Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS / Prisma Access	✗	✓	✓

Vulnerability Details

#1

Palo Alto Networks has warned that a recently disclosed security flaw impacting PAN-OS and Prisma Access is being actively exploited. Tracked as CVE-2026-0257, the vulnerability is a critical authentication bypass issue. The flaw affects the GlobalProtect portal and gateway components of PAN-OS when the authentication override cookie feature is enabled. This feature allows authenticated users to receive encrypted cookies that can be reused instead of repeatedly entering credentials, effectively functioning as bearer tokens. While the feature is not enabled by default and requires manual configuration, affected environments become exposed to significant risk when it is deployed incorrectly.

#2

The vulnerability stems from the way GlobalProtect processes authentication override cookies. When a request containing a portal-userauthcookie or portal-prelogonuserauthcookie value is submitted to the /ssl-vpn/login.esp endpoint, the appliance decrypts the supplied cookie and automatically trusts the resulting content. However, after decryption, the cookie's authenticity is never verified through a digital signature or integrity check. This design flaw allows an attacker with access to the public encryption key to generate a forged cookie that appears legitimate and is subsequently accepted by the server.

#3

Exploitation becomes particularly straightforward when administrators configure the appliance to reuse the same HTTPS service certificate for authentication override cookie encryption and decryption. Because the certificate's public key is exposed during the normal TLS handshake process, an attacker can easily retrieve it from the appliance. Using this public key, a malicious actor can craft forged authentication cookies and submit them to the GlobalProtect portal or gateway. If the correct key is used, the appliance accepts the forged cookie, grants authentication without requiring valid credentials, and in some deployments may even assign a VPN IP address, providing direct access to internal network resources. Researchers have publicly demonstrated this attack path through a proof-of-concept exploit.

#4

Evidence of active exploitation emerged on May 17, 2026, when attackers leveraged forged authentication cookies to access local administrator accounts from infrastructure hosted by Vultr. A second wave of attacks was observed on May 21, 2026, originating from Dromatics Systems infrastructure. Investigators noted that both campaigns used the spoofed MAC address aa:bb:cc:dd:ee, suggesting a common operational pattern. In eight out of ten affected MDR customer environments, attackers successfully authenticated using forged cookies without establishing a complete VPN session, while the remaining incidents resulted in VPN IP assignments. Although no confirmed lateral movement beyond the VPN appliances was observed, the incidents demonstrate that the flaw is being actively weaponized and presents a serious risk to exposed and misconfigured GlobalProtect deployments.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-0257	Palo Alto Networks PAN-OS 10.2 (Before 10.2.7-h34 / 10.2.10-h36 / 10.2.13-h21 / 10.2.16-h7 / 10.2.18-h6), PAN-OS 11.1 (Before 11.1.4-h33 / 11.1.6-h32 / 11.1.7-h6 / 11.1.10-h25 / 11.1.13-h5 / 11.1.15), PAN-OS 11.2 (Before 11.2.4-h17 / 11.2.7-h14 / 11.2.10-h7 / 11.2.12), PAN-OS 12.1 (Before 12.1.4-h6 / 12.1.7), Prisma Access 10.2 (Before 10.2.10-h36), Prisma Access 11.2 (Before 11.2.7-h13)	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	CWE-565

Recommendations

Apply Vendor Patches Immediately: Palo Alto Networks has released patched versions across all affected PAN-OS branches. Organizations running PAN-OS 10.2 should upgrade to 10.2.7-h34, 10.2.10-h36, 10.2.13-h21, 10.2.16-h7, or 10.2.18-h6, depending on their minor version. PAN-OS 11.1 deployments should target 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 deployments should target 11.2.4-h17, 11.2.7-h14, 11.2.10-h7, or 11.2.12. PAN-OS 12.1 deployments should target 12.1.4-h6 or 12.1.7. Prisma Access customers on 10.2 and 11.2 are being actively upgraded per schedule. Note that following the upgrade, GlobalProtect users will be required to re-authenticate once, as a one-time consequence of the cookie regeneration logic introduced in the fix.

Apply Immediate Workarounds if Patching Cannot Be Done Immediately: Organizations unable to patch immediately should apply one of two vendor-recommended mitigations. The first option is to generate a new certificate dedicated exclusively to authentication override cookie encryption and decryption, ensuring it is not shared with the portal or gateway HTTPS service or any other feature. The second and more decisive option is to disable the authentication override feature entirely by unchecking the generate and accept cookie options in the GlobalProtect portal and gateway configuration. Either workaround substantially reduces the exploitability of the vulnerability in the interim.

Verify Configuration Exposure: Administrators should audit their GlobalProtect portal and gateway configurations to determine whether authentication override cookies are enabled and whether the relevant certificate is shared with the HTTPS service. On the portal, this can be checked by navigating to Network > GlobalProtect > Portals, selecting the Agent Configuration profile, and reviewing the Authentication tab for the Generate cookie for authentication override and Accept cookie for authentication override options. On the gateway, administrators should check the Authentication Override tab within the Client Settings profile under the Agent tab.

Investigate for Signs of Active Exploitation: Organizations should review GlobalProtect authentication logs for cookie-based authentications to the local admin account, particularly those originating from unfamiliar source IPs or hosting providers. The presence of successful cookie authentication events from these sources should be treated as a confirmed compromise indicator requiring immediate incident response.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Defense Evasion	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
Lateral Movement	T1021: Remote Services	T1021.005: VPN
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	104[.]207[.]144[.]154, 146[.]19[.]216[.]119, 146[.]19[.]216[.]120, 146[.]19[.]216[.]125
Hostname	GP-CLIENT, DESKTOP-GP01

Patch Link

https://security.paloaltonetworks.com/CVE-2026-0257

References

https://security.paloaltonetworks.com/CVE-2026-0257

https://www.rapid7.com/blog/post/etr-rapid7-observed-exploitation-of-pan-os-globalprotect-authentication-bypass-vulnerability-cve-2026-0257/

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 Demo of **HivePro**.

REPORT GENERATED ON

June 02, 2026 • 8:50 AM

More at www.hivepro.com