AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-0257

Authentifizierungs-Bypass in Palo Alto GlobalProtect.

Ein nicht authentifizierter Angreifer aus dem Internet kann gültige Sitzungs-Cookies fälschen und eine VPN-Verbindung durch Ihr GlobalProtect-Gateway aufbauen – bis hin zu Administrator-Rechten. Voraussetzung ist eine verbreitete Zertifikatskonfiguration; die Ausnutzung ist trivial und läuft seit Mai 2026.

> **Geschäftsrisiko:** unbefugter Fernzugriff auf das interne Netz – mit Potenzial für Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

7,8 / 10

HOCH
CVSS 4.0 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:4.0/AV:N/AC:L/PR:N/UI:N/SC:H/SI:H` – aus dem Netz, ohne Rechte, ohne Zutun, mit hoher Wirkung auf Folgesysteme. Von Palo Alto am 29.05.2026 von 4,7 hochgestuft.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
17. Mai 2026	PAN-OS 10.2–12.1 + Prisma Access	Sofort

Das Wichtigste in 60 Sekunden.

7,8 · HOCH
CVSS-Schweregrad

Auth-Bypass
GlobalProtect Portal & Gateway

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

Cloud NGFW
& Panorama nicht betroffen

Die Ursache: Verwundbare PAN-OS-Versionen vertrauen jedem Auth-Override-Cookie, das sie entschlüsseln können – ohne zu prüfen, ob das Gerät es selbst ausgestellt hat. Wird für den GlobalProtect-HTTPS-Dienst und die Cookie-Verschlüsselung **dasselbe Zertifikat** verwendet, kann ein Angreifer die Zertifikatskette vom öffentlichen Portal abrufen und gültige Cookies für beliebige Nutzer fälschen – inklusive Administrator.

ANGRIFFSKETTE

01	02	03	04
Portal exponiert – GlobalProtect ist aus dem Internet erreichbar	**Zertifikat abgreifen** – Kette vom öffentlichen HTTPS-Dienst laden	**Cookie fälschen** – gültiges Auth-Override-Cookie für jeden Nutzer erzeugen	**Zugang** – VPN-Verbindung als beliebiger Nutzer bis Administrator

Betroffenheit & Fixversionen

PAN-OS-Zweig	Verwundbar bis	Fixversion (Ziel)
10.2	< 10.2.18-h6	10.2.18-h6
11.1	< 11.1.15	11.1.15
11.2	< 11.2.12 (mehrere h-Zweige)	11.2.12
12.1	< 12.1.7 / 12.1.4-h6	12.1.7
Prisma Access	10.2 & 11.2	Rollout mit Palo Alto abstimmen
Cloud NGFW · Panorama	nicht betroffen	—

Angreifbar nur bei aktiven Auth-Override-Cookies **und** gemeinsamem Zertifikat für HTTPS-Dienst und Cookie-Verschlüsselung. Exakte Build-Ranges gegen das Hersteller-Advisory des eigenen Zweigs abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

13.05.2026
Palo Alto veröffentlicht Advisory

17.05.2026
Erste aktive Ausnutzung beobachtet

29.05.2026
CISA KEV · CVSS 4,7 → 7,8 · PoC öffentlich

Seither
In Wellen ausgenutzt – kaum Lateral Movement

Ihr Maßnahmenplan.

In dieser Reihenfolge – Mitigation vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Mitigation aktivieren	Patch einspielen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

In der GlobalProtect-Konfiguration prüfen: Portal/Gateway aktiv? Auth-Override-Cookies eingeschaltet? Dieselbe Zertifikatszuordnung wie beim HTTPS-Dienst? Nur diese Kombination ist angreifbar – Portal und Gateway getrennt kontrollieren.

02 Sofort mitigieren (vor dem Patch)

Eigenes Zertifikat ausschließlich für Auth-Override-Cookies erzeugen – oder das Feature deaktivieren. Von Palo Alto als Behelf bei Phasen-Upgrades benannt:

```
set global-protect enable-auth-override-cookie-hmac no
```

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`10.2.18-h6` · `11.1.15` · `11.2.12` · `12.1.7` bzw. h-Fix). Nach dem Upgrade ist eine Neu-Anmeldung aller Nutzer erwartetes Verhalten – Cookies werden sicher neu erzeugt.

04 Kompromittierung ausschließen

Auth-Logs auf Cookie-Anmeldungen an Admin-/lokalen Konten aus unerwarteten Quellen durchsuchen und die IoCs unten abgleichen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Prisma Access gesondert bewerten

Auch Cloud-basierte Prisma-Access-Umgebungen (10.2 / 11.2) sind betroffen – Patch-/Rollout-Status direkt mit Palo Alto abstimmen. Herstellerseitige Threat-Prevention-/IPS-Signaturen einspielen, sofern für diese Schwachstelle verfügbar.

Kompromittierungs-Indikatoren (IoCs)

LOG-ENDPUNKTE (POST)

`/ssl-vpn/hipreport.esp`
`/ssl-vpn/getconfig.esp`

AUFFÄLLIGE MARKER

Hostnamen `DESKTOP-GP01`, `GP-CLIENT`, `Jocker`
gefälschte MAC `aa:bb:cc:dd:ee:ff`

ANGREIFER-QUELL-IPS

`104.207.144.154` · `209.99.191.137`
`146.19.216.119` / `.120` / `.125`
`79.130.26.202`

Zur Einordnung: Die Log-Endpunkte sind reguläre GlobalProtect-Aufrufe – auffällig nur in Verbindung mit Cookie-Auth an Admin-Konten aus fremden Quellen. IPs und Hostnamen sind eine Momentaufnahme der beobachteten Kampagne und flüchtig – kein Ersatz für die Analyse Ihrer Authentifizierungs-Logs.

Wichtig: Erfolgreiche Anmeldungen erscheinen als reguläre „Cookie"-Authentifizierung an gültigen Konten – ohne Alarm. Ohne kontinuierliche Auswertung der Auth-Logs bleibt ein bereits erfolgter Zugriff unsichtbar.

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

24/7-SOC aus München: Die Cookie-Anmeldung an einem Admin-Konto und anomale VPN-Logins fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte GlobalProtect-Portale über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre PAN-OS-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Mitigation heute anordnen, Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung des Perimeters entscheiden.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch vollständig in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-0257 und dem PAN-OS-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Quellen: Palo Alto Networks Security Advisory CVE-2026-0257 · Rapid7 Emergent Threat Report · Unit 42 Threat Brief · CISA Known Exploited Vulnerabilities Catalog. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.