AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-3400

Unauth. Command Injection in Palo Alto GlobalProtect.

Ein nicht authentifizierter Angreifer aus dem Internet kann über einen manipulierten Sitzungs-Cookie eine Datei auf der Firewall anlegen und darüber beliebige Befehle mit Root-Rechten ausführen. Betroffen sind PAN-OS-Firewalls mit aktivem GlobalProtect-Gateway oder -Portal. Die Lücke wird seit März 2024 im Rahmen der Kampagne „Operation MidnightEclipse" aktiv ausgenutzt.

> **Geschäftsrisiko:** vollständige Übernahme der Perimeter-Firewall mit Root-Rechten – als Sprungbrett ins interne Netz, mit Potenzial für Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

10,0 / 10

KRITISCH
CVSS 4.0 BASISWERT

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/AU:Y/R:U/V:C/RE:M/U:Red`
– aus dem Netz, ohne Rechte, ohne Zutun – Code-Ausführung mit Root-Rechten und voller Wirkung auf das gesamte System. Höchstmöglicher Basiswert 10,0.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
26. März 2024	PAN-OS 10.2 · 11.0 · 11.1 mit GlobalProtect	Sofort

Das Wichtigste in 60 Sekunden.

10,0 · KRITISCH
CVSS-Höchstwert

Root-RCE
unauth. über GlobalProtect

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

Cloud NGFW
Panorama & Prisma Access nicht betroffen

Die Ursache: Verwundbare PAN-OS-Versionen übernehmen den Wert eines Sitzungs-Cookies (`SESSID`) beim GlobalProtect-Dienst ungeprüft als Teil eines Dateinamens. Enthält der Cookie Pfad- und Befehlssyntax, legt die Firewall eine Datei an, deren Name anschließend als Kommando ausgeführt wird (Command Injection, CWE-77 / CWE-20). Es sind weder Anmeldedaten noch Nutzerinteraktion nötig – die Ausführung erfolgt mit **Root-Rechten**.

ANGRIFFSKETTE

01	02	03	04
Portal exponiert – GlobalProtect-Gateway/Portal ist aus dem Internet erreichbar	**Cookie manipulieren** – präparierter `SESSID`-Cookie mit Pfad- und Befehlssyntax an den GlobalProtect-Dienst senden	**Datei anlegen** – Firewall schreibt eine Datei, deren Name die eingeschmuggelten Befehle enthält	**Root-Zugriff** – die Befehle werden als root ausgeführt; Nachladen der UPSTYLE-Backdoor möglich

Betroffenheit & Fixversionen

PAN-OS-Zweig	Verwundbar bis	Fixversion (Ziel)
10.2	< 10.2.9-h1	10.2.9-h1
11.0	< 11.0.4-h1	11.0.4-h1
11.1	< 11.1.2-h3	11.1.2-h3
9.x · 10.0 · 10.1	nicht betroffen	—
Cloud NGFW · Panorama · Prisma Access	nicht betroffen	—

Angreifbar nur bei **aktivem GlobalProtect-Gateway oder -Portal**. Palo Alto hat frühe Hotfix-Builds für alle unterstützten Wartungs-Releases der drei Zweige nachgeliefert – exakte Build-Range gegen das Hersteller-Advisory des eigenen Zweigs abgleichen. Ältere Annahmen zur „Device Telemetry" gelten nicht: die Aktivierung ist für die Angreifbarkeit **nicht** erforderlich.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die Firewall 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

26.03.2024
Erste aktive Ausnutzung (Volexity, UTA0218)

12.04.2024
Palo Alto veröffentlicht Advisory · CISA KEV

14.04.2024
Erste Hotfixes (10.2.9-h1, 11.0.4-h1, 11.1.2-h3)

Seither
Öffentliche PoCs · breite opportunistische Ausnutzung

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

Prüfen: Läuft PAN-OS 10.2, 11.0 oder 11.1? Ist ein GlobalProtect-Gateway oder -Portal konfiguriert und aus dem Internet erreichbar? Nur diese Kombination ist angreifbar – 9.x, 10.0, 10.1 sowie Cloud NGFW, Panorama und Prisma Access sind nicht betroffen.

02 Sofort mitigieren (vor dem Patch)

Für Kunden mit Threat-Prevention-Abo: Vulnerability-Protection mit den Signaturen zu dieser Schwachstelle auf das GlobalProtect-Interface anwenden (Threat-IDs `95187` · `95189` · `95191`). Ist kein Patch sofort möglich, exponierte Portale bis zum Update aus dem Internet nehmen.

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`10.2.9-h1` · `11.0.4-h1` · `11.1.2-h3` oder den passenden früheren Hotfix-Build). Für ältere Wartungs-Releases stehen dedizierte h-Fixes bereit.

04 Kompromittierung ausschließen

Bei potenzieller Exposition Firewall-Logs und Dateisystem auf die unten genannten IoCs prüfen – insbesondere die UPSTYLE-Backdoor und manipulierte `SESSID`-Cookies. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Bei bestätigtem Zugriff: Factory Reset

Bei Anzeichen einer erfolgreichen Ausnutzung empfiehlt Palo Alto eine gründliche Bereinigung (Private-Data-Reset bzw. Factory Reset), da Angreifer persistente Artefakte hinterlassen können. Herstellerseitige Threat-Prevention-Signaturen aktuell halten.

Kompromittierungs-Indikatoren (IoCs)

DIENST-ENDPUNKTE (POST)

`/ssl-vpn/hipreport.esp`
`/global-protect/portal/*`

MANIPULIERTER COOKIE

`SESSID` mit Pfad-/Befehlssyntax (Command Injection über Dateinamen)

UPSTYLE-BACKDOOR (DATEI)

`/var/appweb/sslvpndocs/global-protect/portal/css/bootstrap.min.css`

Zur Einordnung: Die Dienst-Endpunkte sind reguläre GlobalProtect-Aufrufe – auffällig nur in Verbindung mit manipulierten SESSID-Cookies oder untergeschobenen Dateien. Angreifer-IPs und Dateipfade variieren je Kampagne und sind flüchtig – kein Ersatz für die Analyse Ihrer Firewall-Logs und den Abgleich mit dem aktuellen Unit-42-Threat-Brief.

Wichtig: Erfolgreiche Ausnutzung läuft ohne Nutzerinteraktion und mit Root-Rechten – oft unbemerkt. Ein einfacher Patch entfernt eine bereits eingeschleuste Backdoor nicht; bei bestätigter Kompromittierung ist eine vollständige Bereinigung des Geräts erforderlich.

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: Manipulierte SESSID-Cookies und untypische Dateizugriffe auf dem GlobalProtect-Dienst 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 und -Gateways 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 umgehend einplanen (CISA-KEV-Frist war der 19.04.2024).
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Bei bestätigter Kompromittierung Geräte-Bereinigung und dauerhafte Perimeter-Überwachung 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-2024-3400 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-2024-3400 · NVD (CVSS 3.1 10,0; Palo Alto CVSS 4.0 10,0) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 12.04.2024) · Volexity „Zero-Day Exploitation … GlobalProtect (CVE-2024-3400)" · Unit 42 Threat Brief „Operation MidnightEclipse". 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.