AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-9463

Unauth. Command Injection in Palo Alto Expedition.

Ein nicht authentifizierter Angreifer aus dem Netz kann in Palo Altos Migrations-Software Expedition beliebige Betriebssystembefehle mit Root-Rechten ausführen. Dabei lassen sich Nutzernamen, Klartext-Passwörter, Gerätekonfigurationen und API-Schlüssel der angebundenen PAN-OS-Firewalls auslesen. Die Lücke wird seit November 2024 aktiv ausgenutzt und steht im CISA-KEV-Katalog.

> **Geschäftsrisiko:** Diebstahl sämtlicher von Expedition verwalteter Firewall-Zugangsdaten im Klartext und der API-Schlüssel – als Sprungbrett zur Übernahme der Perimeter-Firewalls, mit Potenzial für Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,9 / 10

KRITISCH
CVSS 4.0 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:N/SA:N` – aus dem Netz, ohne Rechte, ohne Zutun – Befehlsausführung mit Root-Rechten und hoher Wirkung auf die von Expedition verwalteten PAN-OS-Firewalls. CVSS 4.0 Basiswert 9,9 (Palo Alto); das NVD führt zusätzlich CVSS 3.1 mit 7,5.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
14. November 2024	Expedition 1 < 1.2.96 PAN-OS-Firewalls mittelbar	Sofort

Das Wichtigste in 60 Sekunden.

9,9 · KRITISCH
CVSS 4.0 · Palo Alto

Root-RCE
unauth. OS-Command-Injection

Aktiv
ausgenutzt · CISA KEV · seit Nov. 2024

Klartext-Passwörter
& API-Keys der Firewalls exponiert

Die Ursache: Expedition übernimmt bei einem aus dem Netz erreichbaren Endpunkt eine vom Angreifer kontrollierte Eingabe ungeprüft in einen Betriebssystem-Befehl (OS Command Injection, CWE-78). Enthält die Eingabe Shell-Metazeichen, führt der Server die eingeschmuggelten Befehle mit **Root-Rechten** aus. Es sind weder Anmeldedaten noch Nutzerinteraktion nötig. Weil Expedition Zugangsdaten und API-Schlüssel der angebundenen PAN-OS-Firewalls im Klartext vorhält, lassen sich diese im selben Zug auslesen.

ANGRIFFSKETTE

01 **Expedition exponiert** – die Weboberfläche des Migrations-Tools ist aus dem Netz erreichbar

02 **Eingabe präparieren** – Anfrage mit Shell-Metazeichen an den verwundbaren Endpunkt senden

03 **Root-Ausführung** – die eingeschmuggelten Befehle laufen als `root`

04 **Credential-Diebstahl** – Nutzernamen, Klartext-Passwörter, Configs und API-Keys der PAN-OS-Firewalls auslesen

Betroffenheit & Fixversionen

Expedition-Version	Verwundbar bis	Fixversion (Ziel)
Expedition 1	`< 1.2.96 (1.2.0–1.2.95)`	`1.2.96`
PAN-OS · Panorama · Prisma Access · Cloud NGFW	nicht direkt betroffen	—

Betroffen ist ausschließlich die Migrations-Software Expedition (Version 1) vor `1.2.96` – nicht PAN-OS, Panorama, Cloud NGFW oder Prisma Access selbst. Da Expedition die Zugangsdaten und API-Schlüssel der verwalteten Firewalls im Klartext verarbeitet, sind diese bei erfolgreicher Ausnutzung **mittelbar kompromittiert**. Palo Alto verlangt, alle über Expedition verarbeiteten Firewall-Zugangsdaten und API-Schlüssel nach dem Update zu rotieren.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf Firewall-Zugangsdaten 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

09.10.2024
Palo Alto veröffentlicht Advisory PAN-SA-2024-0010

14.11.2024
Aktive Ausnutzung gemeldet · Aufnahme in CISA KEV

05.12.2024
CISA-KEV-Umsetzungsfrist für US-Behörden

Seither
Öffentliche Analysen · Angriffe auf exponierte Instanzen

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	ZWINGEND
Expedition abschotten	Patch einspielen	Zugangsdaten rotieren

01 Betroffenheit feststellen

Prüfen: Ist Expedition (Version 1) im Einsatz und läuft eine Version vor `1.2.96`? Ist die Weboberfläche aus dem Netz oder für unberechtigte Hosts erreichbar? Nur diese Kombination ist angreifbar – PAN-OS-Firewalls, Panorama und Prisma Access sind nicht direkt betroffen.

02 Sofort mitigieren (vor dem Patch)

Netzwerkzugriff auf Expedition strikt auf autorisierte Nutzer, Hosts und Netze beschränken. Wird Expedition nicht aktiv genutzt, die Software herunterfahren – beides von Palo Alto als Behelf benannt.

03 Patchen

Auf `Expedition 1.2.96` oder eine neuere Version aktualisieren. Damit ist die Command-Injection geschlossen.

04 Zugangsdaten zwingend rotieren

Palo Alto verlangt ausdrücklich: nach dem Update **alle** Expedition-Zugangsdaten und -API-Schlüssel **und** alle über Expedition verarbeiteten Firewall-Zugangsdaten, Passwörter und API-Schlüssel rotieren. Ein Patch entfernt keine bereits abgeflossenen Credentials.

05 Kompromittierung ausschließen

Host- und Weblogs von Expedition auf anomale Befehlsausführung als `root` und verdächtige Anfragen an die Oberfläche prüfen. Wegen des Root-Zugriffs ist eine gründliche Integritätsprüfung des Systems angeraten – ein Patch schließt die Lücke, nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ZU PRÜFEN (HOST)	WEB-/SYSTEMLOGS	FOLGEINDIKATOR
unerwartete Prozesse / Befehle als `root` auf dem Expedition-Server	Anfragen an die Expedition-Weboberfläche mit `Shell-Metazeichen`	unerwartete Zugriffe auf die gespeicherten Firewall-Credentials / API-Keys

Zur Einordnung: Palo Alto hat für CVE-2024-9463 keine spezifischen netzwerkbasierten IoCs veröffentlicht. Maßgeblich ist die Analyse der Expedition-Host- und Weblogs sowie – wegen des Root-Zugriffs – eine gründliche Integritätsprüfung des Systems. Für die parallel gemeldete Lücke CVE-2024-9465 nennt Palo Alto eine MySQL-Abfrage der cronjobs-Tabelle als Kompromittierungsprüfung.

Wichtig: Da die Befehle mit Root-Rechten laufen, kann ein Angreifer persistente Artefakte hinterlassen und sämtliche in Expedition gespeicherten Firewall-Zugangsdaten im Klartext auslesen. Ein Patch schließt die Lücke – rotieren Sie zwingend alle betroffenen Zugangsdaten und API-Schlüssel.

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: Root-Befehlsausführung auf dem Expedition-Host und anomale Zugriffe auf die Weboberfläche fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte Expedition-Instanzen (< 1.2.96) 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 Expedition-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

- Expedition heute vom offenen Netz trennen bzw. herunterfahren, wenn nicht aktiv genutzt; Update auf 1.2.96 einplanen.
- Alle über Expedition verarbeiteten Firewall-Zugangsdaten und API-Schlüssel rotieren lassen – nicht nur die von Expedition selbst.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung nach NIS-2 / DSGVO.

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-2024-9463 und dem Expedition-Perimeter.

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

Termin buchen

Quellen: Palo Alto Networks Security Advisory PAN-SA-2024-0010 / CVE-2024-9463 · NVD (CVSS 3.1 7,5 HOCH; CVSS 4.0 9,9 KRITISCH; CWE-78) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 14.11.2024, Umsetzungsfrist 05.12.2024). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.