AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-5910

Fehlende Authentifizierung in Palo Alto Expedition.

Eine kritische Funktion in Palo Alto Expedition ist ohne Anmeldung erreichbar. Ein Angreifer mit Netzzugang kann so ein Expedition-Admin-Konto übernehmen – und damit auf die importierten Firewall-Konfigurationen, Klartext-Zugangsdaten und API-Schlüssel zugreifen. In öffentlichen PoCs wird die Lücke mit CVE-2024-9464 zu unauthentifizierter Befehlsausführung verkettet. CISA bestätigt aktive Ausnutzung seit November 2024.

> **Geschäftsrisiko:** Übernahme des zentralen Migrationstools und Abfluss der darin gespeicherten Firewall-Zugangsdaten – mit Potenzial für kompromittierte Firewalls, Datenabfluss und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,3 / 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:L/SI:L/SA:L`
– aus dem Netz erreichbar, ohne Rechte und ohne Zutun ausnutzbar, mit hoher Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit des Systems – und automatisierbar. CVSS 3.1 bewertet die Lücke mit 9,8.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
7. November 2024 (CISA-bestätigt)	Expedition 1.2.0–1.2.91 (Firewall-Migrationstool)	Sofort

Das Wichtigste in 60 Sekunden.

9,3 · KRITISCH
CVSS-Schweregrad

Auth-Bypass
Admin-Übernahme in Expedition

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

Nur Expedition
PAN-OS · Panorama · Prisma nicht betroffen

Die Ursache: Expedition enthält eine kritische Funktion, die **ohne Authentifizierungsprüfung** aufgerufen werden kann (CWE-306). Ein Angreifer mit Netzzugang kann sie ohne Anmeldung nutzen und ein Expedition-Admin-Konto übernehmen. Da Expedition beim Migrieren von Firewall-Konfigurationen Zugangsdaten, API-Schlüssel und weitere Secrets importiert, erhält der Angreifer damit Zugriff auf hochsensible Netz-Geheimnisse. In veröffentlichten Proof-of-Concepts wird die Schwachstelle mit `CVE-2024-9464` zu unauthentifizierter Befehlsausführung auf dem Server verkettet.

ANGRIFFSKETTE

01	02	03	04
Expedition erreichbar – das Migrationstool ist aus dem Netz erreichbar	**Auth umgehen** – ungeschützte kritische Funktion ohne Anmeldung aufrufen	**Admin übernehmen** – Zugriff auf Konfigurationen, Zugangsdaten & API-Schlüssel	**Verkettung → RCE** – mit `CVE-2024-9464` Befehlsausführung auf dem Server

Betroffenheit & Fixversionen

Expedition-Zweig	Verwundbar bis	Fixversion (Ziel)
Expedition 1.2	`< 1.2.92`	`1.2.92`
PAN-OS · Panorama · Prisma Access · Cloud NGFW	nicht betroffen	—

Betroffen ist ausschließlich das eigenständige Migrationswerkzeug **Expedition**, nicht PAN-OS-Firewalls, Panorama oder Prisma Access. Der Fix ist in Expedition `1.2.92` und allen späteren Versionen enthalten – exakte Version gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Da Expedition Firewall-Zugangsdaten und Secrets speichert, kann ein bestätigter Zugriff 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

10.07.2024
Palo Alto veröffentlicht Advisory (PAN-SA-2024-0015) + Fix 1.2.92

Okt. 2024
Horizon3.ai veröffentlicht PoC – Verkettung mit CVE-2024-9464 (RCE)

07.11.2024
CISA KEV · aktive Ausnutzung bestätigt

28.11.2024
CISA-Frist für US-Bundesbehörden

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Netzzugang sperren	Patch einspielen	Secrets rotieren / Threat Hunting

01 Betroffenheit feststellen

Prüfen, ob Expedition im Einsatz ist und welche Version läuft. Jede Version unterhalb `1.2.92` ist angreifbar. Ermitteln, ob die Instanz aus dem Internet oder aus wenig vertrauenswürdigen Netzsegmenten erreichbar ist.

02 Sofort mitigieren (vor dem Patch)

Netzzugang zu Expedition strikt einschränken – nur autorisierte Nutzer, Hosts oder Netze. Von Palo Alto als Behelf benannt. Nicht benötigte Instanzen abschalten, statt sie erreichbar zu lassen.

03 Patchen

Expedition auf `1.2.92` oder neuer aktualisieren. Der Fix schließt die fehlende Authentifizierungsprüfung.

04 Secrets als kompromittiert behandeln

Nach einem bestätigten oder nicht auszuschließenden Zugriff alle über Expedition verarbeiteten Firewall-Zugangsdaten, API-Schlüssel und Secrets als offengelegt betrachten und rotieren. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Abfluss.

05 Kompromittierung ausschließen

Anwendungs- und Systemlogs von Expedition auf unerwartete Admin-Aktivität, Passwort-Resets und Zugriffe aus fremden Quellen prüfen. Auf Anzeichen der Verkettung mit `CVE-2024-9464` (Befehlsausführung durch den Webserver-Nutzer) achten.

Kompromittierungs-Indikatoren (IoCs)

ZUGRIFFE AUF EXPEDITION

Aufrufe der Expedition-Web-App aus dem Internet oder unerwarteten Quellen

ADMIN-KONTO

Unerwartete Passwort-Resets, neue Admin-Sitzungen oder Konfigurationsänderungen

VERKETTUNG → RCE

Shell-/Prozess-Aktivität durch den Webserver-Nutzer (Hinweis auf `CVE-2024-9464`)

Zur Einordnung: Zu dieser Schwachstelle sind öffentlich keine belastbaren netzbasierten IoCs (feste IPs oder Hashes) veröffentlicht. Die Erkennung stützt sich auf Anomalien in den Anwendungs- und Systemlogs von Expedition sowie den Nachweis der Verkettung mit CVE-2024-9464. Kein Ersatz für die Analyse Ihrer eigenen Logs.

Wichtig: Expedition speichert importierte Firewall-Konfigurationen inklusive Klartext-Zugangsdaten und API-Schlüssel. Nach einem bestätigten Zugriff müssen alle darüber verarbeiteten Anmeldedaten und Secrets als kompromittiert gelten und rotiert werden – ein Patch allein genügt nicht.

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: Anomale Zugriffe auf Expedition und unerwartete Admin-Aktivität fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Netz erreichbare, ungepatchte Expedition-Instanzen 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

- Netzzugang zu Expedition heute sperren und auf 1.2.92 aktualisieren.
- Nach bestätigtem Zugriff alle über Expedition verarbeiteten Zugangsdaten, API-Schlüssel und Secrets rotieren – dokumentiert für eine etwaige Meldung.
- Prüfen lassen, ob Expedition dauerhaft benötigt wird; nicht benötigte Instanzen abschalten.

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-2024-5910 und dem Expedition-Perimeter.

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

Termin buchen

Quellen: Palo Alto Networks Security Advisory CVE-2024-5910 (PAN-SA-2024-0015) · NVD (CVSS 4.0 9,3 / CVSS 3.1 9,8, CWE-306) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 07.11.2024) · Horizon3.ai (PoC, Verkettung mit CVE-2024-9464). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.