AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-9465

Unauthentifizierte SQL-Injection in Palo Alto Expedition.

Ein nicht authentifizierter Angreifer aus dem Netz kann über eine SQL-Injection den gesamten Datenbestand des Migrationswerkzeugs Expedition auslesen – Passwort-Hashes, Nutzernamen, Gerätekonfigurationen und Geräte-API-Schlüssel – und beliebige Dateien auf dem System lesen und schreiben. Mit den erbeuteten Zugangsdaten stehen anschließend die verwalteten Firewalls offen. Die Schwachstelle wird seit November 2024 aktiv ausgenutzt.

> **Geschäftsrisiko:** Diebstahl von Firewall-Zugangsdaten und -API-Schlüsseln, in der Folge unbefugter Zugriff auf die verwaltete Netzinfrastruktur – mit Potenzial für Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,2 / 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:L/VA:N/SC:H/SI:N/SA:N` – aus dem Netz, ohne Rechte, ohne Zutun – vollständiger Lesezugriff auf die Expedition-Datenbank inklusive Firewall-Zugangsdaten. CVSS 3.1 bewertet die Lücke mit 9,1.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
14. November 2024	Expedition < 1.2.96	Sofort

Das Wichtigste in 60 Sekunden.

9,2 · KRITISCH
CVSS-Schweregrad (4.0)

Unauth SQLi
ohne Anmeldung auslesbar

Aktiv
ausgenutzt · CISA KEV (seit 14.11.2024)

CWE-89
SQL-Injection

Die Ursache: Expedition validiert in den betroffenen Versionen Eingaben an einem Web-Endpunkt nicht ausreichend, bevor sie in eine SQL-Abfrage einfließen. Ein nicht authentifizierter Angreifer kann dadurch eigene SQL-Befehle in die Datenbank `pandb` einschleusen, deren Inhalt auslesen und über SQL-Dateifunktionen zusätzlich beliebige Dateien auf dem System lesen und schreiben.

ANGRIFFSKETTE

01
Expedition exponiert – das Web-Interface ist über das Netz erreichbar

02
SQL einschleusen – manipulierte, unauthentifizierte Anfrage an den anfälligen Endpunkt

03
Datenbank auslesen – Passwort-Hashes, Nutzernamen, Gerätekonfigurationen und Geräte-API-Schlüssel

04
Ausweitung – Dateien lesen/schreiben und mit erbeuteten Zugangsdaten die verwalteten Firewalls übernehmen

Betroffenheit & Fixversionen

Expedition-Version	Verwundbar bis	Fixversion (Ziel)
Expedition 1.x	< 1.2.96	1.2.96
PAN-OS · Firewalls · Panorama	nicht betroffen	—

Betroffen ist ausschließlich das eigenständige Migrationswerkzeug Expedition in allen Versionen unterhalb 1.2.96. PAN-OS-Firewalls, Panorama und Cloud NGFW sind von dieser Schwachstelle nicht direkt betroffen – wohl aber mittelbar, wenn deren in Expedition gespeicherte Zugangsdaten abgeflossen sind.

Regulatorischer Hinweis: Ein bestätigter Abfluss von Zugangsdaten oder personenbezogenen Daten 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), Fix in 1.2.96

Okt. 2024
Horizon3.ai veröffentlicht technische Analyse und PoC-Details

14.11.2024
CISA nimmt CVE-2024-9465 in den KEV-Katalog auf – aktive Ausnutzung

05.12.2024
KEV-Frist für US-Behörden zum Patchen/Abschalten

Ihr Maßnahmenplan.

In dieser Reihenfolge – Zugriff einschränken, patchen, Zugangsdaten rotieren, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Netzzugriff einschränken / patchen	Zugangsdaten & API-Keys rotieren	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Prüfen, ob Expedition in einer Version unterhalb `1.2.96` im Einsatz und über das Netz erreichbar ist. Expedition ist ein reines Migrationswerkzeug – oft temporär installiert und nach dem Projekt vergessen. Nicht mehr benötigte Instanzen zählen ebenfalls.

02 Sofort mitigieren (vor dem Patch)

Netzzugriff auf Expedition strikt auf autorisierte Nutzer, Hosts und Netze begrenzen. Wird das Werkzeug nicht mehr benötigt, den Dienst abschalten. Von Palo Alto als Behelfsmaßnahme benannt.

03 Patchen

Auf `Expedition 1.2.96` oder neuer aktualisieren. Damit ist die SQL-Injection geschlossen.

04 Zugangsdaten als kompromittiert behandeln

Da die Datenbank Passwort-Hashes, Nutzernamen und Geräte-API-Schlüssel enthält, alle in Expedition gespeicherten Firewall- und Admin-Zugangsdaten sowie API-Schlüssel rotieren – ein Patch macht bereits abgeflossene Geheimnisse nicht ungültig.

05 Kompromittierung ausschließen

Die von Palo Alto genannte Prüfung auf ungewöhnliche Datenbank-Cronjobs ausführen und Web-/Zugriffslogs auf anomale Anfragen an das Expedition-Interface durchsuchen.

```
mysql -uroot -p -D pandb -e "SELECT * FROM cronjobs;"
```

Kompromittierungs-Indikatoren (IoCs)

KOMPROMITTIERUNGS-CHECK

Ungewöhnliche Einträge in `pandb.cronjobs`
`SELECT * FROM cronjobs;`

AUFFÄLLIGE AKTIVITÄT

Unauthentifizierte Anfragen an das Expedition-Web-Interface aus fremden Quellen

FOLGEINDIKATOREN

Neu-/Fremdanmeldungen an Firewalls oder Panorama mit in Expedition hinterlegten Konten

Zur Einordnung: Die Cronjob-Prüfung ist der von Palo Alto genannte konkrete Kompromittierungshinweis. Da die eigentliche SQL-Injection über reguläre Web-Anfragen läuft, ist sie ohne detaillierte Zugriffs-Logs schwer zu erkennen – der zuverlässigste Indikator ist die Auswertung Ihrer Web- und Firewall-Authentifizierungs-Logs.

Wichtig: Der Kern des Risikos liegt nicht in Expedition selbst, sondern in den dort gespeicherten Geheimnissen: Sind Firewall-Zugangsdaten und API-Schlüssel einmal abgeflossen, bleibt der Zugang auch nach dem Patch bestehen. Deshalb ist die Rotation aller betroffenen Zugangsdaten ebenso wichtig wie das Update.

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 Anfragen an das Expedition-Interface und die Nutzung darüber abgeflossener Firewall-Zugangsdaten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden 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

- Netzzugriff auf Expedition heute einschränken oder den Dienst abschalten; Patch auf 1.2.96 unverzüglich einplanen.
- Alle in Expedition gespeicherten Firewall- und Admin-Zugangsdaten sowie API-Schlüssel rotieren lassen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.

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-2024-9465 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-2024-9465 / PAN-SA-2024-0010 · NVD (CVSS 4.0: 9,2 / CVSS 3.1: 9,1, CWE-89) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 14.11.2024) · Horizon3.ai Attack Research. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.