AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-0012

Authentifizierungs-Bypass im PAN-OS Management-Interface.

Ein nicht authentifizierter Angreifer mit Netzzugang zum PAN-OS-Management-Webinterface kann die Anmeldung vollständig umgehen und Administrator-Rechte erlangen – ohne gültige Zugangsdaten. Ursache ist eine fehlende Authentifizierung an einer kritischen Funktion (CWE-306). Die Lücke wird seit November 2024 aktiv ausgenutzt, häufig verkettet mit der Rechteausweitung CVE-2024-9474.

> **Geschäftsrisiko:** vollständige administrative Übernahme von Firewall bzw. Panorama – mit Potenzial für Konfigurationsmanipulation, Umgehung der Perimeter-Kontrollen, Zugriff auf das interne Netz, Persistenz 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:N/SA:N/E:A/AU:N/R:U/V:C/RE:H/U:Red` – aus dem Netz, ohne Rechte, ohne Zutun – volle Wirkung auf das betroffene System. Palo Alto vergibt den Basiswert 9,3 (CVSS 4.0) und weist die Exploit-Reife „aktiv ausgenutzt" (E:A) aus; das NVD führt zusätzlich den CVSS-3.1-Basiswert 9,8.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
November 2024	PAN-OS 10.2 · 11.0 · 11.1 · 11.2 Firewalls & Panorama	Sofort

Das Wichtigste in 60 Sekunden.

9,3 · KRITISCH	Pre-Auth-Bypass	Aktiv	CWE-306
CVSS-Schweregrad (4.0)	Management-Webinterface	ausgenutzt · CISA KEV (seit 18.11.2024)	fehlende Authentifizierung

Die Ursache: Das PAN-OS-Management-Webinterface prüft für eine kritische Funktion die Authentifizierung nicht ausreichend (CWE-306: Missing Authentication for Critical Function). Ein entfernter, nicht authentifizierter Angreifer mit Netzzugang zum Interface kann die Anmeldung damit vollständig umgehen und **PAN-OS-Administrator-Rechte** erlangen. Von dort lassen sich administrative Aktionen ausführen, die Konfiguration verändern oder weitere authentifizierte Schwachstellen – insbesondere die Rechteausweitung `CVE-2024-9474` – nachgelagert ausnutzen.

ANGRIFFSKETTE

01	02	03	04
Interface exponiert – das PAN-OS-Management-Webinterface ist aus dem Netz erreichbar	**Auth umgehen** – ohne gültige Zugangsdaten wird die Anmeldung übergangen (CWE-306)	**Admin-Rechte** – der Angreifer agiert mit PAN-OS-Administrator-Berechtigung	**Verkettung** – nachgelagert oft `CVE-2024-9474` für Codeausführung/Root

Betroffenheit & Fixversionen

PAN-OS-Zweig	Verwundbar bis	Fixversion (Ziel)
10.2	< `10.2.12-h2`	`10.2.12-h2`
11.0	< `11.0.6-h1`	`11.0.6-h1`
11.1	< `11.1.5-h1`	`11.1.5-h1`
11.2	< `11.2.4-h1`	`11.2.4-h1`
Cloud NGFW · Prisma Access	nicht betroffen	—

Betroffen sind PA-Series-, VM-Series- und CN-Series-Firewalls sowie Panorama (virtuell & M-Series). **Cloud NGFW und Prisma Access sind nicht betroffen.** Praktisch angreifbar ist nur ein aus dem Netz erreichbares Management-Webinterface. Exakte Build-Ranges gegen das Hersteller-Advisory des eigenen Zweigs abgleichen.

Regulatorischer Hinweis: Eine bestätigte administrative Übernahme bzw. ein 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

08.11.2024	14.11.2024	18.11.2024	09.12.2024	Seither
Palo Alto veröffentlicht Vorab-Hinweis PAN-SA-2024-0015 (Management-Interface abschotten)	Palo Alto stuft die Bedrohung hoch – aktive Angriffe beobachtet	CVE-2024-0012 veröffentlicht, Fixes bereitgestellt · CISA KEV · PoC öffentlich	CISA-Frist für US-Bundesbehörden (BOD 22-01)	Fortlaufende Ausnutzung, häufig verkettet mit CVE-2024-9474

Ihr Maßnahmenplan.

In dieser Reihenfolge – Management-Interface abschotten vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Management-Zugriff einschränken	Patch einspielen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

PAN-OS-Version prüfen (10.2 / 11.0 / 11.1 / 11.2 – gegen die Tabelle abgleichen) und feststellen, ob das Management-Webinterface aus dem Internet oder aus nicht vertrauenswürdigen Netzen erreichbar ist. Cloud NGFW und Prisma Access sind nicht betroffen. Nur ein exponiertes Management-Interface ist praktisch angreifbar.

02 Sofort mitigieren (vor dem Patch)

Herstellerbehelf: Zugriff auf das Management-Interface ausschließlich auf vertrauenswürdige interne IP-Adressen beschränken und es niemals aus dem Internet erreichbar machen. Das reduziert die Angriffsfläche deutlich, bis der Patch eingespielt ist.

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`10.2.12-h2` · `11.0.6-h1` · `11.1.5-h1` · `11.2.4-h1` und höher). Palo Alto hat für alle betroffenen Zweige feste Builds veröffentlicht.

04 Threat Prevention aktivieren

Sofern lizenziert, die herstellerseitigen Threat-IDs `95746` · `95747` · `95752` · `95753` · `95759` · `95763` (Applications-and-Threats-Content 8915-9075 und höher) einspielen, um Angriffsversuche zu blockieren.

05 Kompromittierung ausschließen

Da die Lücke häufig mit `CVE-2024-9474` verkettet wird: Logs auf unerwartete administrative Aktionen, neue/geänderte Admin-Konten und Konfigurationsänderungen sowie auf hinterlegte Web-Shells prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

EXPONIERTER DIENST

PAN-OS-Management-Webinterface aus dem Internet / aus nicht vertrauenswürdigen Netzen erreichbar

THREAT-PREVENTION-SIGNATUREN

Threat-IDs `95746` · `95747` · `95752` · `95753` · `95759` · `95763` (Content `8915-9075+`)

KONFIGURATIONS-DRIFT

unautorisierte Admin-Aktionen, neue/geänderte Admin-Konten, Konfigurationsänderungen und hinterlegte Web-Shells (Verkettung mit CVE-2024-9474)

Zur Einordnung: Die Threat-IDs sind herstellerbestätigte Blocking-Signaturen; die Verhaltensmarker sind allgemeine Prüfhinweise und kein Ersatz für die Analyse Ihrer Management-, Zugriffs- und Systemlogs. Ein erfolgreicher Bypass erscheint als reguläre administrative Aktivität – ohne Auswertung der Logs bleibt ein erfolgter Zugriff unsichtbar.

Wichtig: Ein erfolgreicher Auth-Bypass gewährt volle Administrator-Rechte und erscheint als reguläre administrative Aktivität. In Verkettung mit CVE-2024-9474 folgt Codeausführung mit Root-Rechten. Ein reiner Patch entfernt bereits etablierte Persistenz, geänderte Konfiguration oder Konten nicht – ohne Prüfung des Systems bleibt eine erfolgte Kompromittierung 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: administrative Aktionen ohne vorangegangene Anmeldung und anomale Zugriffe auf das Management-Interface fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte PAN-OS-Management-Interfaces 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

- Management-Zugriff heute auf vertrauenswürdige interne IPs beschränken, Patch kurzfristig (CISA-Frist war 09.12.2024) einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – inklusive Verkettung mit CVE-2024-9474 –, dokumentiert für eine etwaige Meldung.
- Grundsatz durchsetzen: Management-Interfaces von Sicherheitsgeräten nie direkt exponieren.

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-2024-0012 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-2024-0012 (PAN-SA-2024-0015) · NVD (nvd.nist.gov, CVSS 4.0 Basiswert 9,3 / CVSS 3.1 9,8, CWE-306) · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 18.11.2024, Frist 09.12.2024). 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.