AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-9474

Root-Befehlsausführung im PAN-OS Management-Interface.

Über die Web-Verwaltungsoberfläche von PAN-OS lassen sich Befehle mit Root-Rechten auf der Firewall ausführen. Für sich genommen setzt die Lücke einen Verwaltungszugang voraus – in freier Wildbahn wird sie jedoch mit dem Authentifizierungs-Bypass CVE-2024-0012 verkettet, sodass ein nicht angemeldeter Angreifer aus dem Internet die vollständige Kontrolle über das Gerät erlangt. Die Ausnutzung läuft seit dem 18. November 2024.

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

6,9 / 10

MITTEL
CVSS 4.0 BASISWERT

Niedrig | **Mittel** | Hoch | Kritisch

`CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N/AU:N/R:U/V:C/RE:H/U:Red`
– aus dem Netz, mit vorhandenem Verwaltungszugang, ohne Nutzerzutun – erlaubt beliebige Befehle mit Root-Rechten auf der Firewall. In der Praxis mit dem Auth-Bypass CVE-2024-0012 zu voller, unauthentifizierter Geräteübernahme verkettet. CVSS 3.1: 7,2 (HOCH).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
18. November 2024	PAN-OS 10.1–11.2 Management-Interface	Sofort

Das Wichtigste in 60 Sekunden.

6,9 · MITTEL
CVSS 4.0 (3.1: 7,2 · HOCH)

Root-RCE
über Management-Web-Interface

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

Verkettet
mit Auth-Bypass CVE-2024-0012

Die Ursache: Die Web-Verwaltungsoberfläche von PAN-OS reicht Eingaben ungeprüft in einen Betriebssystem-Befehl weiter (OS Command Injection, CWE-78). Ein angemeldeter Administrator kann so Kommandos mit **Root-Rechten** ausführen. Der nötige Verwaltungszugang entfällt in der Praxis, weil Angreifer die Lücke mit dem Authentifizierungs-Bypass **CVE-2024-0012** verketten und dadurch ohne gültige Zugangsdaten auf das Management-Interface gelangen.

ANGRIFFSKETTE

01
Interface exponiert – PAN-OS-Management-Web-Oberfläche ist aus dem Internet erreichbar

02
Auth umgehen – CVE-2024-0012 verschafft unauthentifizierten Zugriff auf das Management-Interface

03
Root-Befehl – CVE-2024-9474 führt Kommandos mit Root-Rechten aus

04
Persistenz – PHP-Webshell, Open-Source-C2-Tools und Krypto-Miner nachgeladen

Betroffenheit & Fixversionen

PAN-OS-Zweig	Verwundbar bis	Fixversion (Ziel)
10.1	< 10.1.14-h6	10.1.14-h6
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	—

Das Advisory nennt je Zweig zahlreiche freigegebene Hotfix-Builds; die angegebenen Fixversionen sind die empfohlenen Ziel-Builds. Betroffen sind nur Geräte mit erreichbarem PAN-OS-Management-Web-Interface. Exakte Build-Ranges des eigenen Zweigs gegen das Hersteller-Advisory abgleichen.

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

18.11.2024
Palo Alto Advisory · CISA KEV · erste Ausnutzung

19.11.2024
Technische Details öffentlich – Angriffe nehmen zu

20.11.2024
Unit 42 „Operation Lunar Peek": Webshells, C2, Miner

09.12.2024
CISA-Frist für US-Bundesbehörden

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Management-Interface abschotten	Patch einspielen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

PAN-OS-Version je Zweig prüfen und feststellen, ob das Management-Web-Interface aus dem Internet oder aus nicht vertrauenswürdigen Netzen erreichbar ist. Nur exponierte, ungepatchte Geräte sind praktisch gefährdet.

02 Sofort mitigieren (vor dem Patch)

Zugriff auf das Management-Interface ausschließlich auf vertrauenswürdige interne IP-Adressen beschränken und jede Erreichbarkeit aus dem Internet unterbinden – der vom Hersteller genannte Behelf. Zusätzlich die für diese Schwachstelle bereitgestellten Threat-Prevention-/IPS-Signaturen aktivieren, sofern lizenziert.

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`10.1.14-h6` · `10.2.12-h2` · `11.0.6-h1` · `11.1.5-h1` · `11.2.4-h1` bzw. den passenden Hotfix-Build). CVE-2024-0012 wird durch dieselben Versionen geschlossen – beide Lücken gemeinsam beheben.

04 Kompromittierung ausschließen

Gerät auf hinterlassene PHP-Webshells, unerwartete Konfigurationsänderungen, neue Cron-Jobs und Management-Zugriffe aus fremden Quellen untersuchen. Ein Tech-Support-File zur forensischen Auswertung sichern. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Kette bewerten

Die reale Gefahr entsteht aus der Verkettung mit dem Auth-Bypass `CVE-2024-0012`. Beide CVEs stehen in der CISA-KEV-Liste; die Absicherung des Management-Perimeters ist die wirksamste dauerhafte Gegenmaßnahme.

Kompromittierungs-Indikatoren (IoCs)

WEB-SHELL (SHA-256)

```
3c5f9034c86cb1952aa5bb07b4f77ce7
d8bb5cc9fe5c029a32c72adc7e814668
```

AUFFÄLLIGER USER-AGENT

```
Mozilla/5.0 (Windows NT 6.3;
Trident/7.0; rv 11.0) like
Gecko
```

ANGREIFER-QUELLEN

Zugriffe über anonyme VPN-/Proxy-Dienste; laufend gepflegte IP-Liste im Unit-42-Threat-Intel-Repository

Zur Einordnung: Der Zugriff auf das Management-Interface ist regulärer Administrations-Verkehr – auffällig nur aus fremden Quellen oder nach dem Auth-Bypass. Hashes, User-Agent und IPs sind eine Momentaufnahme der beobachteten Kampagne und flüchtig – kein Ersatz für die forensische Prüfung des Geräts.

Wichtig: Nach der Übernahme agiert der Angreifer mit Root-Rechten auf der Firewall selbst – Webshells und C2-Kanäle laufen unterhalb üblicher Netzwerk-Alarme. Ohne forensische Prüfung des Geräts bleibt ein bereits erfolgter Zugriff 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: Unerwartete Root-Kommandos und neue Dateien auf der Firewall sowie Management-Zugriffe aus fremden Quellen fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden PAN-OS-Firewalls mit aus dem Internet erreichbarem Management-Interface 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-Interface heute vom Internet trennen; Patch für CVE-2024-9474 und CVE-2024-0012 innerhalb der CISA-Frist einspielen.
- Firewalls forensisch auf Webshells und unautorisierte Änderungen prüfen lassen – dokumentiert für eine etwaige Meldung.
- Grundsatz durchsetzen: keine Verwaltungsoberflächen im offenen Internet.

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-2024-9474 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-2024-9474 · NVD (NIST) CVE-2024-9474 · CISA Known Exploited Vulnerabilities Catalog (hinzugefügt 18.11.2024, Frist 09.12.2024) · Unit 42 „Operation Lunar Peek". 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.