AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-0111

Authentifizierter Datei-Zugriff im PAN-OS Management-Interface.

Wer sich am PAN-OS-Management-Interface anmelden kann, kann beliebige vom Systemkonto „nobody" lesbare Dateien vom Firewall-Dateisystem auslesen – etwa Konfigurationen und Geheimnisse. Für sich genommen braucht es gültige Zugangsdaten; in freier Wildbahn wird die Lücke jedoch mit dem Authentifizierungs-Bypass CVE-2025-0108 verkettet, sodass ein nicht angemeldeter Angreifer aus dem Netz denselben Datei-Zugriff erhält – aktiv beobachtet seit Februar 2025.

Geschäftsrisiko: Abfluss sensibler Firewall-Daten (Konfiguration, Schlüsselmaterial, Anmeldedaten) als Sprungbrett zur vollständigen Übernahme des Geräts – mit Potenzial für Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

7,1 / 10

HOCH
CVSS 4.0 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:A/AU:N/R:U/V:C/RE:M/U:Red`
– aus dem Netz, geringe Komplexität, mit niedrigen Rechten (eine gültige Anmeldung am Management-Interface genügt), ohne Zutun – mit hoher Wirkung auf die Vertraulichkeit. CVSS 3.1 stuft die Lücke isoliert als 6,5 (Mittel) ein.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
18. Februar 2025	PAN-OS 10.1 · 10.2 · 11.1 · 11.2 Cloud NGFW & Prisma Access nicht betroffen	Sofort

Das Wichtigste in 60 Sekunden.

7,1 · HOCH
CVSS 4.0 Basiswert

Datei-Read
Management-Interface (PAN-OS)

Aktiv
ausgenutzt · CISA KEV · verkettet

Cloud NGFW
& Prisma Access nicht betroffen

Die Ursache: Das Management-Web-Interface von PAN-OS erlaubt einem angemeldeten Nutzer, über einen extern kontrollierbaren Datei-/Pfad-Verweis (CWE-73 / CWE-610) Dateien vom lokalen Dateisystem zu lesen, die dem Dienstkonto „nobody" zugänglich sind. Dazu zählen sensible Inhalte wie Konfigurationsdateien. In den beobachteten Angriffen wird diese Lücke mit dem Authentifizierungs-Bypass CVE-2025-0108 kombiniert – die eigentlich nötige Anmeldung entfällt damit.

ANGRIFFSKETTE

01
Interface exponiert – das PAN-OS-Management-Interface ist aus dem Netz erreichbar

02
Auth-Bypass – CVE-2025-0108 umgeht die Anmeldung am Management-Interface

03
Datei-Read (CVE-2025-0111) – vom „nobody"-Konto lesbare Dateien werden ausgelesen, z. B. Konfiguration & Geheimnisse

04
Eskalation – verkettet mit CVE-2024-9474 bis zu Root-Rechten und vollständiger Geräteübernahme

Betroffenheit & Fixversionen

PAN-OS-Zweig	Verwundbar bis	Fixversion (Ziel)
10.1	< 10.1.14-h9	10.1.14-h9
10.2	< 10.2.13-h3 (mehrere h-Zweige)	10.2.13-h3
11.1	< 11.1.6-h1 (mehrere h-Zweige)	11.1.6-h1
11.2	< 11.2.4-h4 / < 11.2.5	11.2.5
Cloud NGFW · Prisma Access	nicht betroffen	—

Alle nicht gepatchten PAN-OS-Versionen der genannten Zweige sind betroffen; End-of-Life-Versionen gelten als angreifbar. Exakte Build-Ranges gegen das Hersteller-Advisory des eigenen Zweigs abgleichen. Cloud NGFW und Prisma Access sind laut Hersteller nicht betroffen.

Regulatorischer Hinweis: Ein bestätigter Abfluss von Firewall-Konfiguration oder Anmeldedaten 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

12.02.2025
Palo Alto veröffentlicht Advisory
CVE-2025-0111 · Überblick

18.02.2025
Aktive Ausnutzung beobachtet – verkettet mit CVE-2025-0108 / CVE-2024-9474

20.02.2025
Aufnahme in den CISA-KEV-Katalog

21.02.2025
Fixversionen für 11.1 / 11.2 verfügbar

06.03.2025
Letztes Advisory-Update – EoL-Versionen bestätigt

Seite 3: Ihre Maßnahmenplan offen

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Management-Zugriff einschränken	Patch einspielen	Threat Hunting / Log-Analyse

01 Betroffenheit feststellen

PAN-OS-Version je Zweig prüfen und mit den Fixversionen abgleichen. Entscheidend ist zusätzlich: Ist das Management-Interface aus dem Netz oder aus nicht vertrauenswürdigen Segmenten erreichbar? Nur dann ist das Angriffsrisiko akut.

02 Sofort mitigieren (vor dem Patch)

Zugriff auf das Management-Interface ausschließlich auf vertrauenswürdige interne IP-Adressen beschränken – nie aus dem Internet erreichbar. Herstellerseitige Threat-Prevention-Signaturen aktivieren (Threat-IDs `510000` und `510001`, Applications-and-Threats-Content v8943 oder neuer).

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`10.1.14-h9` · `10.2.13-h3` · `11.1.6-h1` · `11.2.5`). End-of-Life-Zweige (u. a. 11.0) erhalten keinen Fix – hier ist ein Upgrade auf einen unterstützten Zweig erforderlich.

04 Kompromittierung ausschließen

Da die Lücke mit dem Auth-Bypass CVE-2025-0108 verkettet wird, die Management-Plane-Zugriffslogs auf unerwartete Datei-Aufrufe und Zugriffe aus fremden Quellen prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Bei Verdacht: Geheimnisse rotieren

Wurde ein Zugriff festgestellt, gemäß Hersteller den Master-Key wechseln, Passwörter, Pre-Shared-Keys und API-Schlüssel zurücksetzen sowie ausgestellte Zertifikate widerrufen und neu ausstellen.

Kompromittierungs-Indikatoren (IoCs)

ANGRIFFSVEKTOR

Zugriffe auf das `PAN-OS-Management-Interface` mit Datei-/Pfad-Parametern, die einen Datei-Read auslösen

VERKETTUNG

Anfragen ohne vorausgegangene erfolgreiche Anmeldung (Auth-Bypass `CVE-2025-0108`) – gefolgt von Datei-Read und ggf. `CVE-2024-9474`

QUELLEN

Management-Zugriffe aus `nicht vertrauenswürdigen / externen IP-Bereichen`

Zur Einordnung: Für diese Schwachstelle liegen keine belastbaren statischen IoCs (feste IPs/Hashes) vor – die Analyse Ihrer Management-Plane-Zugriffslogs ist maßgeblich. Angreifer nutzen das reguläre Management-Interface; auffällig sind unerwartete Datei-Aufrufe und Zugriffe aus fremden Quellen.

Wichtig: Für sich genommen erfordert die Lücke gültige Zugangsdaten – der reale Angriff umgeht diese Hürde jedoch über den Auth-Bypass CVE-2025-0108. Ein exponiertes Management-Interface ist damit auch ohne Anmeldung angreifbar; ohne Log-Auswertung bleibt ein erfolgter Datei-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: Datei-Read-Aufrufe am Management-Interface und 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 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-Interface heute vom Netz nehmen bzw. auf vertrauenswürdige IPs beschränken, Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Bei Zugriffsverdacht Geheimnisse rotieren und über dauerhafte Perimeter-Überwachung entscheiden.

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-2025-0111 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-2025-0111 · NVD (nvd.nist.gov/vuln/detail/CVE-2025-0111) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 20.02.2025, Frist 13.03.2025). 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.