AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-0300

Ungepatchte PAN-OS-Firewalls: Root-Übernahme über das User-ID Captive Portal.

Eine Buffer-Overflow-Schwachstelle (CWE-787) im User-ID Authentication Portal – dem Captive Portal – von PAN-OS erlaubt es einem nicht authentifizierten Angreifer, per präparierter Pakete beliebigen Code mit Root-Rechten auf der Firewall auszuführen. Palo Alto bestätigt aktive Ausnutzung gegen Portale, die aus dem Internet oder untrusted Netzen erreichbar sind. Fixes liegen für alle betroffenen Branches vor; exponierte, ungepatchte Systeme müssen sofort behandelt werden.

Geschäftsrisiko: Die Firewall ist das Perimeter-Gerät: Eine Root-Übernahme gibt dem Angreifer die Kontrolle über den gesamten Netzwerkverkehr, ermöglicht Datenabfluss, dauerhafte Persistenz und dient als Sprungbrett ins interne Netz – ein typischer Einstiegspunkt für Ransomware.

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:N/E:A/AU:Y/R:U/V:C/RE:M/U:Red`
– Über das Netzwerk, ohne Anmeldung und mit geringem Aufwand ausnutzbar; führt zu vollständiger Codeausführung mit Root-Rechten auf der Firewall.

AUSGENUTZT SEIT
6. Mai 2026

BETROFFEN
Betroffen sind PA-Series- und VM-Series-Firewalls mit aktivem User-ID Authentication Portal (Captive Portal) in den Branches 10.2, 11.1, 11.2 und 12.1.
Nicht betroffen: Prisma Access, Cloud NGFW und Panorama.

HANDLUNGSBEDARF
Zeitnah

Das Wichtigste in 60 Sekunden.

9,3	Root	0	KEV
CVSS 4.0 (Kritisch)	Rechte bei erfolgreicher RCE	Authentifizierung nötig	aktiv ausgenutzt

Die Ursache: Der Dienst des User-ID Authentication Portals (Captive Portal) validiert die Länge eingehender Daten unzureichend, wodurch ein Out-of-bounds Write (CWE-787) entsteht. Speziell präparierte Pakete überschreiben Speicher im Portal-Prozess und erlauben die Ausführung von Angreifer-Code mit Root-Rechten. Voraussetzung ist ein erreichbares, aktiviertes Portal – besonders kritisch bei Exposition gegenüber Internet oder untrusted Zonen.

ANGRIFFSKETTE

01	02	03	04
Präparierte Pakete an das exponierte User-ID Authentication Portal (Captive Portal) senden.	**Buffer Overflow** im Portal-Dienst: Out-of-bounds Write (CWE-787) überschreibt Speicher.	**Root-Codeausführung** ohne jede Authentifizierung direkt auf der Firewall.	**Perimeter-Übernahme**: Traffic-Manipulation, Persistenz und Pivot ins interne Netz.

Betroffenheit & Fixversionen

Feste Version	Verwundbar bis	Fixversion (Ziel)
PAN-OS 12.1	< 12.1.7	12.1.7
PAN-OS 11.2	< 11.2.12	11.2.12
PAN-OS 11.1	< 11.1.15	11.1.15
PAN-OS 10.2	< 10.2.18-h6	10.2.18-h6

Palo Alto liefert je Wartungszweig eigene Hotfixes; wer auf einem älteren Maintenance-Train bleibt, nutzt die passende Fix-Version dieses Trains (z. B. 12.1.4-h5, 11.2.7-h13, 11.2.10-h6, 11.1.4-h33, 11.1.6-h32, 11.1.10-h25, 11.1.13-h5, 10.2.10-h36, 10.2.13-h21, 10.2.16-h7). Auch Siemens RUGGEDCOM APE1808 (mit PAN-OS) ist betroffen (Siemens SSA-967325). Genaue Zuordnung stets im Hersteller-Advisory prüfen.

Regulatorischer Hinweis: NIS-2: aktiv ausgenutzte, kritische Schwachstelle am Perimeter – meldepflichtige Sicherheitsvorfälle sind ohne zeitnahes Patchen wahrscheinlich, die Frühwarn-/Meldefristen (24/72 h) greifen. DSGVO: Bei Kompromittierung droht Zugriff auf personenbezogene Daten – Art. 33/34 (Meldung binnen 72 h, ggf. Betroffenenbenachrichtigung) beachten.

ZEITACHSE

06.05.2026
Palo Alto veröffentlicht Advisory; aktive Ausnutzung bestätigt

06.05.2026
Aufnahme in CISA KEV (Known Exploited Vulnerabilities)

14.07.2026
Heute: Fixes verfügbar – ungepatchte, exponierte Systeme bleiben akut gefährdet

Ihr Maßnahmenplan.

Vom Exposure-Check über Sofort-Mitigation bis zum verifizierten Patch – priorisiert nach Internet-Exposition des Captive Portals.

SOFORT	24-48 H	7 TAGE
Exposition prüfen; Captive Portal aus dem Internet/untrusted Zonen nehmen bzw. mitigieren	Patch auf die feste Version des jeweiligen Branches einspielen	Kompromittierungs-Check und dauerhaftes Perimeter-Hardening abschließen

01 Betroffenheit prüfen

Feststellen, ob das User-ID Authentication Portal (Captive Portal) aktiv und aus untrusted Zonen bzw. dem Internet erreichbar ist. Betroffen sind nur PA-/VM-Series mit aktivem Portal.

```
show running security-policy | match auth-portal
```

02 Sofort mitigieren

Portal-Zugriff auf trusted Zonen beschränken und Response Pages im Interface Management Profile aller L3-Interfaces mit untrusted Ingress deaktivieren. Threat-Prevention-Kunden aktivieren Threat ID 510019 (PAN-OS 11.1+).

03 Patchen

Auf die feste Version des jeweiligen Branches aktualisieren (12.1.7 / 11.2.12 / 11.1.15 / 10.2.18-h6 bzw. den passenden Maintenance-Hotfix).

04 Kompromittierung ausschließen

System- und Portal-Logs, Prozessliste und Konfiguration auf unbekannte Admins, Config-Änderungen oder Dienst-Abstürze prüfen (siehe Unit 42 Threat Brief).

05 Exposition dauerhaft senken

Management- und Portal-Dienste nicht ins Internet exponieren; Monitoring/Alarme auf den Firewall-Dienst schärfen.

⚠ **Wichtig:** Aktiv ausgenutzt und im CISA-KEV: Eine erfolgreiche Ausnutzung liefert Root ohne Authentifizierung. Exponierte, ungepatchte Portale sind mit höchster Dringlichkeit zu behandeln – Mitigation sofort, Patch binnen 24-48 h.

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: Auffällig im SOC: wiederholte Abstürze/Neustarts des Captive-Portal-Dienstes, ungewöhnliche oder überlange Pakete an den Portal-Port, unerwartete Root-Prozesse oder Konfigurationsänderungen auf der Firewall sowie ausgehende Verbindungen vom Firewall-Management. 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-Firewalls mit aktivem User-ID Authentication Portal (Captive Portal) 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 Palo Alto-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

- Sofortige Priorisierung: alle PA-/VM-Series mit aktivem Captive Portal identifizieren und internet-exponierte Portale unverzüglich schließen oder mitigieren.
- Patch-Deployment auf die festen Versionen innerhalb von 24-48 h; Fortschritt und Restrisiko wöchentlich berichten.
- Kompromittierungs-Check für exponierte Geräte beauftragen; NIS-2-/DSGVO-Meldepflichten vorsorglich vorbereiten.

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-2026-0300 und dem Palo Alto-Perimeter.

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

Termin buchen