

PREPARE PROTECT DETECT RESPOND IMPROVE

● AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-0322

Code Injection im PAN-OS-Management: Root auf Firewall und Panorama mit Admin-Zugang.

Über das Management-Interface von PAN-OS kann ein Angreifer mit administrativem Zugang eigenen Code einschleusen und mit Root-Rechten ausführen – auf PA- und VM-Series-Firewalls sowie Panorama. Palo Alto hat die Lücke am 14. Oktober 2026 mit Fixversionen veröffentlicht und meldet sehr begrenzte Ausnutzung; CISA hat sie am selben Tag in den KEV-Katalog aufgenommen – mit forensischer Triage-Pflicht. Einen Workaround gibt es nicht.

Geschäftsrisiko: vollständige Übernahme der Firewall bzw. der Panorama-Verwaltung – mit Kontrolle über Regelwerk, VPN-Zugänge und Perimeter-Verkehr, als Sprungbrett ins interne Netz; ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO ist dann wahrscheinlich.

8,6 / 10

HOCH

CVSS 4.0 BASISWERT



CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/AU:N/R:U/V:D/RE:M/U:Red
– aus dem Netz, mit geringem Aufwand und ohne Zutun eines Nutzers – aber nur mit hohen (administrativen) Rechten am Management; volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Basiswert von Palo Alto als CNA; bei nur angrenzend erreichbarem Management 8,5, NVD (CVSS 3.1) 7,2.

AUSGENUTZT SEIT

spätestens 14.10.2026

BETROFFEN

PAN-OS 10.2 – 12.2 · Panorama
Fix: 12.2.4 · 12.1.10-h2 · 11.2.16 u. a.

HANDLUNGSBEDARF

Sofort

Das Wichtigste in 60 Sekunden.

8,6 · HOCH

CVSS 4.0 (Palo Alto) · NVD 3.1: 7,2

Code Injection

Management-Interface · Root · CWE-94

Aktiv

ausgenutzt · CISA KEV · Frist 17.10.2026

Patch da

alle Zweige · kein Workaround



Die Ursache: PAN-OS prüft über das **Management-Interface** nicht ausreichend, welche Eingaben eines angemeldeten Administrators in ausführbaren Code einfließen (**Code Injection, CWE-94**). Wer sich mit Admin-Rechten anmelden kann, schleust eigene Befehle ein – und die laufen **mit Root-Rechten** auf dem Betriebssystem von Firewall bzw. Panorama. Besonders kritisch, wenn das Management aus dem Internet oder nicht vertrauenswürdigen Netzen erreichbar ist.

ANGRIFFSKETTE

01 Management erreichbar – Management-Interface aus dem Netz zugänglich	02 Admin-Zugang – Anmeldung mit hohen Rechten, etwa über erbeutete oder schwache Zugangsdaten	03 Code eingeschleust – präparierte Eingabe wird als Code verarbeitet (CWE-94)	04 Root-Ausführung – Kontrolle über Firewall bzw. Panorama, Persistenz und Pivot
---	---	--	--

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
PAN-OS 12.2	< 12.2.4	12.2.4
PAN-OS 12.1	< 12.1.10-h2	12.1.10-h2
PAN-OS 11.2	< 11.2.16	11.2.16
PAN-OS 11.1	< 11.1.16-h3	11.1.16-h3
PAN-OS 10.2	< 10.2.18-h12	10.2.18-h12

Genannt ist je Zweig der jüngste Fixstand; für ältere Wartungsstände gibt es passende Hotfixes (z. B. 12.1.7-h8 · 11.2.13-h3 · 11.1.13-h15 · 10.2.16-h11) – vollständige Liste im Hersteller-Advisory. 11.2.16 wurde am 15.10.2026 nachgereicht. Nicht mehr unterstützte Versionen erhalten keinen Fix. Prisma Access und Cloud NGFW sind nicht betroffen.



Regulatorischer Hinweis: Eine übernommene Firewall oder Panorama-Instanz ist in der Regel ein meldepflichtiger Sicherheitsvorfall – NIS-2 nach den für Sie geltenden Fristen, DSGVO bei personenbezogenen Daten unverzüglich (i. d. R. 72 h). Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung, Forensik und Dokumentation.

ZEITACHSE

14.10.2026

Advisory mit Fixversionen

14.10.2026

CISA-KEV · Frist 17.10.2026

15.10.2026

Fix 11.2.16 nachgereicht

17.10.2026

CISA-Frist abgelaufen

Ihr Maßnahmenplan.

In dieser Reihenfolge – Managementzugriff sofort eingrenzen, Patch zügig, Prüfung vor Entwarnung.

SOFORT

Management nur aus vertrauenswürdigen Netzen

KURZFRISTIG

Auf den Fixstand des eigenen Zweigs aktualisieren

PARALLEL

Kompromittierung ausschließen

01

Betroffenheit feststellen

PAN-OS-Stand aller Firewalls und Panorama-Instanzen erheben und mit der Fixtabelle abgleichen. Prüfen, aus welchen Netzen das Management-Interface erreichbar ist – Internet-Erreichbarkeit hat höchste Priorität.

`show system info | match sw-version`

02

Sofort eingrenzen (vor dem Patch)

Einen Workaround gibt es nicht. Managementzugriff auf vertrauenswürdige interne IP-Adressen bzw. eine Jump-Box beschränken. Threat-Prevention-Kunden können die Threat IDs 510046 und 510047 nutzen – nur mit Management über DP-Port, SSL-Entschlüsselung und begrenzter Abdeckung.

03

Patchen

Auf 12.2.4 · 12.1.10-h2 · 11.2.16 · 11.1.16-h3 · 10.2.18-h12 oder den passenden Hotfix des eigenen Wartungsstands aktualisieren – Panorama eingeschlossen. Vorher Konfigurationssicherung ziehen.

04

Kompromittierung ausschließen

Der Patch schließt die Tür – er wirft niemanden hinaus, der schon drin ist. Admin-Anmeldungen und Konfigurationsänderungen auf unbekannte Quell-IPs, neue Admin-Konten und unerwartete Commits prüfen, Logs mit den IoCs abgleichen. CISA verlangt eine forensische Triage.

05

Admin-Zugänge als offengelegt behandeln

Die Lücke setzt Admin-Rechte voraus: Passwörter und API-Schlüssel der Administratoren erneuern, MFA für das Management erzwingen – und bei Verdacht Beweise sichern, bevor das Gerät neu aufgesetzt wird.

Kompromittierungs-Indikatoren (IoCs)

ANGREIFER-IP-ADRESSEN

66.42.72.14
208.83.239.114
149.248.47.234

SIGNATUREN

Threat IDs 510046 / 510047
ab Content 9159-10287

LOG-PRÜFHINWEISE

Admin-Anmeldungen von unbekannten Quell-IPs,
neue Admin-Konten oder API-Schlüssel,
Commits ohne Change-Ticket

Zur Einordnung: Die IP-Adressen und Threat IDs stammen aus dem Palo-Alto-Advisory; dateibasierte Indikatoren hat der Hersteller nicht veröffentlicht. Die Log-Prüfhinweise sind allgemeine Ableitungen aus dem Angriffsweg, keine bestätigten Indikatoren. Infrastruktur ist trivial änderbar – belastbarer ist die Frage, wer sich wann von wo am Management angemeldet hat.



Wichtig: Die Lücke braucht einen Admin-Zugang – wer ausnutzt, sieht im Log aus wie ein Administrator. Wer nur fehlgeschlagene Anmeldungen überwacht, sieht die Übernahme nicht; ein Patch allein beweist nicht, dass niemand drin ist.

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: Admin-Anmeldungen am Firewall-Management von untypischen Quell-IPs oder zu untypischen Zeiten sowie Konfigurationsänderungen und neue Admin-Konten ohne Change 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 und Panorama-Instanzen, deren Management-Interface aus dem Internet oder aus nicht vertrauenswürdigen Netzen erreichbar ist 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

- › Heute anordnen: Management aller Palo-Alto-Firewalls und Panorama-Instanzen nur noch aus vertrauenswürdigen internen Netzen erreichbar machen.
- › Fixversionen zügig einspielen und Admin-Zugangsdaten erneuern – Fortschritt bis zum Abschluss berichten lassen.
- › Für Geräte mit bisher erreichbarem Management eine forensische Prüfung beauftragen – 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-2026-0322 und dem Palo Alto-Perimeter.

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



Termin buchen