AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-3393

Firewall-Ausfall durch DNS-Paket in Palo Alto PAN-OS.

Ein nicht authentifizierter Angreifer aus dem Internet kann mit einem einzigen präparierten DNS-Paket Ihre PAN-OS-Firewall zum Neustart zwingen. Wiederholte Pakete treiben das Gerät in den Wartungsmodus – die Firewall fällt aus und muss manuell wiederhergestellt werden. Voraussetzung ist aktives DNS Security mit eingeschaltetem Logging; die Schwachstelle wird bereits ausgenutzt.

> **Geschäftsrisiko:** Ausfall der Firewall und damit der Netzanbindung bzw. des Perimeter-Schutzes – mit Potenzial für Betriebsunterbrechung und einen meldepflichtigen Verfügbarkeitsvorfall nach NIS-2.

8,7 / 10

HOCH
CVSS 4.0 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L/E:A/AU:N/R:U/V:C/RE:M/U:Amber`
– aus dem Netz, ohne Rechte, ohne Zutun, mit hoher Auswirkung auf die Verfügbarkeit. Ausnutzung wird bereits beobachtet. CVSS 3.1 liegt bei 7,5.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Dezember 2024	PAN-OS 10.1–11.2 mit DNS Security + Logging	Sofort

Das Wichtigste in 60 Sekunden.

8,7 · HOCH	DoS / Reboot	Aktiv	Cloud NGFW & Panorama
CVSS-Schweregrad	Firewall-Datenebene	ausgenutzt · CISA KEV	nicht betroffen

Die Ursache: Die DNS-Security-Funktion prüft eingehende DNS-Pakete beim Protokollieren nicht ausreichend auf ungültige oder unerwartete Zustände (CWE-754). Ein speziell präpariertes, bösartiges DNS-Paket, das durch die Datenebene läuft und protokolliert wird, löst einen Neustart der Firewall aus. Angreifbar ist nur, wer eine DNS-Security- oder Advanced-DNS-Security-Lizenz einsetzt **und** das DNS-Security-Logging aktiviert hat.

ANGRIFFSKETTE

01	02	03	04
Voraussetzung – DNS Security lizenziert und Logging aktiviert	**Paket senden** – präpariertes DNS-Paket läuft durch die Datenebene	**Neustart** – die fehlerhafte Protokollierung erzwingt einen Reboot	**Wartungsmodus** – wiederholte Pakete legen die Firewall dauerhaft lahm

Betroffenheit & Fixversionen

PAN-OS-Zweig	Verwundbar bis	Fixversion (Ziel)
10.1	10.1.14 bis < 10.1.14-h8 / < 10.1.15	10.1.14-h8 · 10.1.15
10.2	10.2.8 bis < 10.2.14 (diverse h-Zweige)	10.2.14 bzw. h-Fix
11.1	< 11.1.5 (diverse h-Zweige)	11.1.5 bzw. h-Fix
11.2	< 11.2.3	11.2.3
Prisma Access	betroffene PAN-OS-Versionen	Rollout mit Palo Alto abstimmen
Cloud NGFW · Panorama · 10.0 / 9.1	nicht betroffen	—

Angreifbar nur bei aktiver DNS-Security-Lizenz **und** eingeschaltetem DNS-Security-Logging. Innerhalb von 10.2 sind erst Builds ab 10.2.8, innerhalb von 10.1 erst ab 10.1.14 betroffen. Exakte Build-Ranges des eigenen Zweigs gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Ein Ausfall der Firewall-Infrastruktur kann als erhebliche Störung der Verfügbarkeit nach NIS-2 meldepflichtig sein – Fristen nach den für Sie geltenden Vorgaben. Ein Datenabfluss und damit die DSGVO sind hier in der Regel nicht einschlägig; der Ausfall von Schutzsystemen kann jedoch Folgerisiken erzeugen. Die Bewertung bleibt bei Ihnen; wir unterstützen bei Einordnung und Dokumentation.

ZEITACHSE

27.12.2024	27.12.2024	30.12.2024	Seither
Palo Alto veröffentlicht Advisory CVE-2024-3393 · Überblick	Aktive DoS-Fälle bei Kunden bekannt	Aufnahme in CISA KEV · Frist 20.01.2025	Fixversionen und Mitigation verfügbar

Seite 3: Ihr Maßnahmenplan →

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Mitigation aktivieren	Patch einspielen	Verfügbarkeit prüfen

01 Betroffenheit feststellen

Prüfen, ob eine DNS-Security- oder Advanced-DNS-Security-Lizenz aktiv ist und das DNS-Security-Logging eingeschaltet ist. Verwundbar sind Konfigurationen, deren Log-Level nicht auf „none" steht:

```
show config merged | match log-level
```

02 Sofort mitigieren (vor dem Patch)

In den Anti-Spyware-Profilen die Log-Severity für **alle** DNS-Security-Kategorien auf „none" setzen. Vordefinierte Profile („Default"/„Strict") lassen sich nicht ändern – dafür einen benutzerdefinierten Klon anlegen und in den betroffenen Sicherheitsregeln hinterlegen. Von Palo Alto als Behelf benannt.

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`10.1.15` · `10.2.14` · `11.1.5` · `11.2.3` bzw. den passenden h-Fix). Nach dem Patch kann das DNS-Security-Logging wieder aktiviert werden.

04 Verfügbarkeit sicherstellen

Prüfen, ob Firewalls bereits von unerwarteten Neustarts betroffen waren oder in den Wartungsmodus (Maintenance Mode) gewechselt sind. Ein Gerät im Wartungsmodus erfordert manuelles Eingreifen und ist bis dahin ausgefallen.

05 Prisma Access gesondert bewerten

Prisma-Access-Umgebungen auf betroffenen PAN-OS-Versionen sind ebenfalls angreifbar – Patch-/Rollout-Status direkt mit Palo Alto abstimmen. Cloud NGFW und Panorama sind nicht betroffen.

Kompromittierungs-Indikatoren (IoCs)

SYSTEM-SIGNAL	PRÜFBEFEHL	BETROFFENE FUNKTION
`unerklärte Firewall-Neustarts` Eintritt in den Wartungsmodus (Maintenance Mode)	`show config merged | match log-level` verwundbar, wenn nicht `log-level none;`	`DNS Security` mit aktivem Logging im Anti-Spyware-Profil

Zur Einordnung: Für diese Schwachstelle sind keine belastbaren Netzwerk-IoCs (IPs/Payloads) öffentlich bestätigt – das primäre Signal ist der DoS selbst: die Reboot-Schleife und der Wartungsmodus. Die Angriffspakete laufen durch die reguläre Datenebene und fallen im Netzverkehr nicht ohne Weiteres auf.

Wichtig: Eine Reboot-Schleife nimmt die Firewall vom Netz – mit ihr fällt der Perimeter-Schutz für das dahinterliegende Netz aus. Der Wartungsmodus erfordert manuelles Eingreifen; ohne Überwachung der Geräteverfügbarkeit bleibt ein Ausfall unbemerkt, bis Dienste ausfallen.

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: Wiederholte, unerklärte Firewall-Neustarts und der Eintritt in den Wartungsmodus fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden Firewalls mit aktivem DNS Security und eingeschaltetem DNS-Security-Logging 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

- Mitigation (DNS-Security-Logging auf „none") heute anordnen, Patch innerhalb der CISA-Frist einplanen.
- Prüfen lassen, ob Firewalls bereits von Neustarts oder Wartungsmodus betroffen waren – dokumentiert für eine etwaige NIS-2-Meldung.
- Über eine dauerhafte Überwachung der Geräteverfügbarkeit am Perimeter 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-2024-3393 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-2024-3393 · NVD (nvd.nist.gov) · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 30.12.2024, Frist 20.01.2025). 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.