



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Palo Alto Networks Firewalls: Aktive Ausnutzung einer ungepatchten Schwachstelle

CSW-Nr. 2024-231856-1332, Version 1.3, 24.04.2024

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 12. April 2024 veröffentlichte das Unternehmen Palo Alto Networks ein Advisory [PALO24a] zu einer aktiv ausgenutzten Schwachstelle in PAN-OS, dem Betriebssystem der Firewalls des Herstellers. Bei der Sicherheitslücke mit der Kennung CVE-2024-3400 handelt es sich um eine OS Command Injection im GlobalProtect Gateway Feature, die einem unauthentifizierten Angreifenden aus der Ferne das Ausführen von Code mit Root-Rechten auf der Firewall ermöglicht. Die Schwachstelle wurde nach dem Common Vulnerability Scoring System (CVSS) mit dem höchsten Wert 10.0 ("kritisch"; CVSS 4.0) bewertet.

Betroffen von der Schwachstelle CVE-2024-3400 sind Firewalls mit:

- PAN-OS 11.1 mit Version < 11.1.2-h3
- PAN-OS 11.0 mit Version < 11.0.4-h1
- PAN-OS 10.2 mit Version < 10.2.9-h1

mit konfiguriertem GlobalProtect Gateway und aktiviertem Telemetrie-Feature.

Sollte eine der genannten Konfigurationen nicht aktiviert sein, so ist keine Ausnutzung möglich.

Die älteren Versionen von PAN-OS (10.1, 10.0, 9.1 und 9.0), die Cloud-Lösung NGFW, Panorama Appliances und Prisma Access sind nicht betroffen.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.

2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.

3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.

4 / Rot: Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Die **Patches** (11.1.2-h3, 11.0.4-h1, 10.2.9-h1) werden nach Angaben im Advisory [PALO24a] voraussichtlich am **14. April 2024 veröffentlicht**.

Palo Alto Networks gibt an, eine **begrenzte Anzahl an Angriffen mittels dieser Schwachstelle** beobachtet zu haben.

Update 1:

Am 15. April 2024 gab der Hersteller die Hotfixes 11.1.2-h3, 11.0.4-h1 und 10.2.9-h1 für PAN-OS 11.1.2, 11.0.4 bzw. 10.2.9 heraus, welche die Schwachstelle schließen [PALO24a]. Hotfixes für weitere PAN-OS Versionen sollen in den nächsten Tagen folgen.

Das IT-Sicherheitsunternehmen Volexity veröffentlichte letzte Woche einen Blogbeitrag [VOLX24] zur beobachteten Ausnutzung von CVE-2024-3400. Dort enthalten sind Details zum Vorgehen der Angreifenden sowie Indikatoren einer Kompromittierung. Demnach konnte Volexity feststellen, dass die Angreifenden bereits am 26. März 2024 erfolgreiche Ausnutzungsversuche bei mehreren Organisationen durchführten. Am 10. April 2024 konnten diese erstmals erfolgreich schadhafte Payload auf den Firewalls installieren. Diese nutzten sie daraufhin, um mit weiteren Tools Zugangsdaten zu entwenden und sich auf interne Netzwerke auszubreiten (Lateral Movement).

Einen weiteren Blogbeitrag zu diesem Sachverhalt mit technischen Details und Indikatoren veröffentlichte das Threat-Intelligence Team Unit42 [UNIT42].

Update 2:

Palo Alto Networks hat das Advisory [PALO24a] angepasst und weist darauf hin, dass der **bisherige Workaround**, das Deaktivieren der Telemetrie-Funktion, **nicht** mehr vor dem Ausnutzen der Schwachstelle CVE-2024-3400 **schützt**. Des Weiteren wird eine zunehmend **breite Ausnutzung beobachtet** und Exploits sind öffentlich verfügbar.

Update 3:

Neben den physischen Geräten von Palo Alto können auch Produkte anderer Hersteller, welche die verwundbaren PAN-OS Versionen (beispielsweise als virtuelle Maschine) integriert und Global Protect konfiguriert haben, anfällig sein. Hiervon berichtet Siemens in seinem Security Advisory SSA-750274 [SIEM24].

Nach Scans der Shadowserver Foundation sind in Deutschland weiterhin mehr als 130 durch CVE-2024-3400 kompromittierte Firewalls zu finden (Stand 23.04.2024) [SHAD24].

Bewertung

Firewalls stellen eine der grundlegenden Sicherheitskomponenten für IT-Netzwerke dar. Eine Kompromittierung oder ein Ausfall können gravierende Auswirkungen auf Vertraulichkeit, Verfügbarkeit und Integrität zur Folge haben und zu massiven Beeinträchtigungen von Geschäftsprozessen führen.

Somit sind Firewalls hochwertige Ziele für Angreifende, um Zugriff auf interne Netzwerke zu erhalten und weiterführende Angriffe zu initiieren.

Aufgrund der bereits beobachteten Attacken ist mit einer zeitnahen breitflächigen Ausnutzung ungeschützter Firewalls zu rechnen, weshalb Maßnahmen sofort ergriffen werden müssen.

Update 1:

Volexity geht von einem technisch versierten Angreifenden aus, der es (vorerst) auf einzelne Ziele abgesehen hatte. Nach dem öffentlichen Bekanntwerden wurden jedoch ein anderes Vorgehen und **breite Angriffe** beobachtet. Die Angreifenden konnten sich zudem auf interne Netzwerke ausbreiten.

Es ist wichtig, dass Betreiber von Palo Alto Network Firewalls diese gründlich auf eine mögliche, bereits stattgefundenene Kompromittierung prüfen und auf Auffälligkeiten überwachen.

Update 2:

Bislang ungepatchte Systeme sind durch die breite Ausnutzung der Schwachstelle sowie dem nicht länger schützenden Workaround stark gefährdet. Das Deaktivieren der Telemetrie-Funktion schützt nicht vor Angriffen. Eine Prüfung auf eine Kompromittierung ist daher notwendig.

Update 3:

Produkte anderer Hersteller, die die verwundbare Software integriert haben, sind leichter zu übersehen. Es besteht somit das Risiko, dass eine erfolgreiche Kompromittierung länger nicht erkannt wird.

Maßnahmen

Zum aktuellen Zeitpunkt stehen noch keine Patches zur Verfügung. Diese sind für den 14. April 2024 angekündigt.

Betreiber sollten schnellstmöglichst prüfen, ob Sie von der Schwachstelle betroffen sind. Dazu kann in der Weboberfläche unter Network > GlobalProtect > Gateways geprüft werden, ob "GlobalProtect Gateway" konfiguriert sowie unter Device > Setup > Telemetry, ob das Telemetry-Feature aktiviert ist. Sollte dies der Fall sein, so muss einer der Workarounds angewandt werden.

Palo Alto empfiehlt zwei Workarounds, mit denen die Zeit bis zur Verfügbarkeit der Updates überbrückt werden kann:

Option 1:

Institutionen sollten das Telemetry-Feature an betroffenen Geräten deaktivieren [PALO24b], bis auf eine nicht-~~verwundbare~~ Version von PAN-OS aktualisiert wird. Nach der Installation des Updates muss die Telemetry-Option ~~händisch wieder eingeschaltet~~ werden.

Option 2:

Institutionen, die Palo Altos Threat Prevention-Dienstleistung nutzen, können Angriffe durch Aktivierung der Threat ID 95187 blockieren. Zusätzlich muss Vulnerability Protection auf dem GlobalProtect Interface aktiviert werden [PALO24c].

Zur Prüfung, ob die Firewall bereits kompromittiert wurde, gibt Palo Alto Networks im Customer Support Portal (CSP) die Möglichkeit, ein "technical support file" (TSF) hochzuladen und damit auf eine Ausnutzung der Schwachstelle prüfen zu lassen [PALO24a].

IT-Sicherheitsverantwortliche sollten die Verfügbarkeit des angekündigten Sicherheitsupdates in den kommenden Tagen regelmäßig kontrollieren und dieses nach Veröffentlichung zeitnah installieren. Institutionen, die bislang nicht betroffene, ältere Versionen von PAN-OS einsetzen, sollten die Aktualisierung der Firewalls nach Bereitstellung der angekündigten Updates ebenfalls grundsätzlich in Betracht ziehen.

Update 1:

Mit den Hotfixes 11.1.2-h3, 11.0.4-h1 und 10.2.9-h1 hat der Hersteller inzwischen Sicherheitsupdates für erste PAN-OS Versionen herausgegeben. Weitere Fixes für andere Releases sollen in den kommenden Tagen folgen. IT-Sicherheitsverantwortliche aus Organisationen, die bislang andere PAN-OS Versionen einsetzen, sollten [PALO24a] daher regelmäßig auf die Veröffentlichung weiterer Updates prüfen.

Institutionen, in denen als Workaround die o.g. Option 1 umgesetzt wurde, weist der Hersteller zusätzlich darauf hin, dass – sofern Firewalls zentral über Palo Altos Panorama verwaltet werden – eine Anpassung in den Panorama Templates erfolgen muss [PALO24d].

Betreiber von Palo Alto Networks Firewalls sollten diese auf eine Kompromittierung hin prüfen. Hierzu wurden von Volexity verschiedene Detektionsmöglichkeiten veröffentlicht. Unter anderem durch die Analyse des Netzwerkdatenverkehrs und über Logs ("technical support file") kann eine erfolgte Ausnutzung festgestellt werden. Weitere Detektionsmöglichkeiten sollen jedoch zeitnah im Blogbeitrag veröffentlicht werden. [VOLX24]

Cortex XDR Kunden können außerdem über XQL Abfragen (siehe [UNIT42]) nach Indikatoren auf ihren Firewalls suchen.

Ebenfalls sollten die IOCs von Volexity [GITH24] und Unit42 gesichtet und zur Prüfung verwendet werden. Yara-Regeln stehen dort ebenfalls zur Verfügung.

Das BSI empfiehlt bei Auffälligkeiten alle Zugangsdaten zu tauschen.

Sollte eine Kompromittierung erkannt worden sein, so ist es wichtig, die Firewall NICHT ohne Sicherung aller forensischen Daten (u.a. Logs) zurückzusetzen. Ebenfalls sollte von einem Ausbreiten der Angreifer auf interne Netzwerke sowie Kompromittierung (u.a. auf der Firewall) gespeicherter Zugangsdaten ausgegangen werden. Sie können sich bei Verdacht an den Palo Alto Networks Support wenden.

Update 2:

Betreiber von Palo Alto Networks Firewalls, die bislang nur den Workaround (Option 1) - Deaktivierung des Telemetrie Features - angewandt haben, sollten schnellstmöglich einen der verfügbaren Hotfixes installieren, da der ursprünglich empfohlene Workaround wirkungslos ist. [PALO24a]

Weiterhin wurden weitere Hotfixes veröffentlicht:

PAN-OS 10.2:

- 10.2.9-h1, 10.2.8-h3, 10.2.7-h8, 10.2.6-h3, 10.2.5-h6

PAN-OS 11.0:

- 11.0.4-h1, 11.0.3-h10, 11.0.2-h4

PAN-OS 11.1:

- 11.1.2-h3, 11.1.1-h1, 11.1.0-h3

Zusätzliche Versionen folgen in den nächsten Tagen (siehe [PALO24a]).

Das Advisory wurde zudem um eine Detektionsmöglichkeit einer Kompromittierung ergänzt:

Hierzu muss in der PAN-OS CLI der Befehl:

```
| grep pattern "failed to unmarshal session(\\.+\\.\\/" mp-log gpsvc.log*
```

ausgeführt werden, um nach *"failed to unmarshal session"* Error-Logs zu suchen. Diese Einträge sehen üblicherweise wie folgt aus:

```
| "message":"failed to unmarshal session(01234567-89ab-cdef-1234-567890abcdef)"
```

Wenn der Wert zwischen "session(" und ")" nicht wie eine GUID (siehe im Beispiel) aussieht, sondern einen Dateisystem-Pfad enthält, deutet dies auf eine Ausnutzung von CVE-2024-3400 hin. Es sind in diesem Fall weitere Untersuchungen notwendig.

Für Institutionen, die Palo Altos Threat Prevention-Dienstleistung einsetzen, wurden ebenfalls weitere Thread IDs veröffentlicht 95187, 95189, und 95191 (siehe [PALO24a]).

Der Blogbeitrag von Unit42 [UNIT42] wurde außerdem um weitere IOCs erweitert.

Update 3:

Konkrete Hinweise, wie Produkte anderer Hersteller, die die verwundbare Software integriert haben, abzusichern sind, können den Security Advisories der Hersteller entnommen werden. Dem BSI liegt keine Liste der betroffenen Lösungen vor. IT-Sicherheitsverantwortliche sollten bei Recherchen zu den in der eigenen Institution genutzten Produkten prüfen, ob hier PAN-OS integriert und Global Protect konfiguriert werden (können).

Im Rahmen seiner gesetzlichen Befugnisse informiert das BSI Betreiber kompromittierter IT-Systeme inzwischen auch über CERT-Bund-Reports. Diese Maßnahmen garantieren jedoch keine Identifikation sämtlicher Angriffsaktivitäten und entbinden Institutionen nicht von ihren Pflichten im Sinne des Patchmanagements.

Weitere Informationen zur sicheren Nutzung von Firewalls können dem BSI IT-Grundschutz entnommen werden [BSI24].

Links

[PALO24a] Palo Alto Networks Security Advisories - CVE-2024-3400

<https://security.paloaltonetworks.com/CVE-2024-3400>

[PALO24b] Disable Device Telemetry

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/device-telemetry/device-telemetry-configure/device-telemetry-disable>

[PALO24c] Applying Vulnerability Protection to GlobalProtect Interfaces

<https://live.paloaltonetworks.com/t5/globalprotect-articles/applying-vulnerability-protection-to-globalprotect-interfaces/ta-p/340184>

[BSI24] BSI IT-Grundschutz: NET.3.2 Firewall (Edition 2023)

<https://www.bsi.bund.de/dok/1073490>

Update 1:

[VOLX24] Zero-Day Exploitation of Unauthenticated RCE Vulnerability in GlobalProtect

<https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/>

[UNIT42] Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400

<https://unit42.paloaltonetworks.com/cve-2024-3400/>

[PALO24d] Panorama Administrator's Guide

<https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/add-a-template>

[GITH24] Volexity IOCs

<https://github.com/volexity/threat-intel/blob/main/2024/2024-04-12%20Palo%20Alto%20Networks%20GlobalProtect/indicators/iocs.csv>

Update 3:

[SIEM24] SSA-750274: Impact of CVE-2024-3400 on RUGGEDCOM APE1808 devices configured with Palo Alto Networks Virtual NGFW

<https://cert-portal.siemens.com/productcert/html/ssa-750274.html>

[SHAD24] Shadowserver Dashboard - CVE-2024-3400

https://dashboard.shadowserver.org/statistics/combined/map/?map_type=std&day=2024-04-23&source=http_vulnerable&source=http_vulnerable6&tag=cve-2024-3400%2B&geo=all&data_set=count&scale=log

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1. Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2. Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
- **TLP:GREEN: Organisationsübergreifende Weitergabe**
Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
 - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
- **TLP:RED: Persönlich, nur für benannte Empfänger**
Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3. Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4. Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.