Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Palo Alto Networks Firewalls: Aktive Ausnutzung einer ungepatchten Schwachstelle

CSW-Nr. 2024-231856-1032, Version 1.0, 12.04.2024

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** beobachtete zu haben.

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.

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 Telementrie-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 Telemetrie-Feature an betroffenen Geräten deaktivieren [PALO24b], bis auf eine nicht-verwundbare Version von PAN-OS aktualisiert wird. Nach der Installation des Updates muss die Telemetrie-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.

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

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.