Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Palo Alto Networks Firewalls: Zero-Day Angriffe auf Management Interface beobachtet

CSW-Nr. 2024-291133-1132, Version 1.1, 19.11.2024

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 14. November aktualisierte Palo Alto Networks ein Advisory [PALO24a] auf seiner Webseite. Nachdem der Hersteller dort erst wenige Tage zuvor eine mögliche Gefährdung durch eine Sicherheitslücke in seinem Firewall-Management Interface bekanntgegeben hatte, wies er nun darauf hin, dass inzwischen Angriffe auf verwundbare Geräte stattfinden. Demnach habe man eine begrenzte Anzahl an Attacken auf Firewalls, die das Management Interface exponieren, bestätigen können. Die Dringlichkeit des Sachverhalts wurde daher auf die höchste Stufe angehoben.

Angreifende nutzen dabei eine Schwachstelle aus, die es erlaubt, ohne Authentifizierung Befehle auszuführen. Die Sicherheitslücke wird nach dem Common Vulnerability Scoring System (CVSS Version 4.0) mit einer Kritikalität von 9.3 ("kritisch") bewertet. Eine Kennung (CVE) ist bislang nicht verfügbar.

Zum aktuellen Zeitpunkt gibt der Hersteller keine Details über die betroffenen Versionen bzw. Geräte an. Es sollen jedoch alle Modelle, die das Management Interface nicht nach Best Practices absichern und daher nach außen exponieren, potentiell gefährdet sein. Palo Alto Networks geht allerdings davon aus, dass zumindest Prisma Access sowie Cloud NGFW nicht betroffen sind. [PALO24a]

Bislang existiert kein Patch zum Schutz vor den beobachteten Angriffen, der Zugriff auf das Management Interface muss unbedingt eingeschränkt werden.

* 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.

Palo Alto Networks hat selbst nach exponierten Geräten im Internet gescannt. Kunden können in ihrem Support Account prüfen, ob von ihnen betriebene Systeme dabei auffällig geworden sind.

Update 1:

Am 18. November kam es zu einer weiteren Aktualisierung des Advisories durch Palo Alto Networks. Dieses Mal ergänzte der Hersteller Hinweise auf die **Verfügbarkeit von Patches**, eine CVE-Kennung der ausgenutzten Sicherheitslücken und weitere Details zum Sachverhalt.

Demnach erlaubt die Schwachstelle CVE-2024-0012 externen, nicht-authentifizierten Angreifenden mit Zugriff auf das Management Interface die Durchführung von Aktionen mit administrativen Rechten und so die Konfiguration bzw. Manipulation der Firewall. Grund für die Verwundbarkeit ist eine fehlende Authentifizierung für eine kritische Funktion (CWE-306).

Außerdem nutzten die Angreifenden eine zweite Schwachstelle mit der Kennung CVE-2024-9474 aus, um root-Rechte zu erlangen [PALO24c].

CVE-2024-0012 wird nach dem Common Vulnerability Scoring System in Version 4.0 (CVSS 4.0) hinsichtlich des Schweregrads mit 9.3 als "kritisch", CVE-2024-9474 mit 6.9 als "medium" klassifiziert.

Sowohl CVE-2024-0012 als auch CVE-2024-9474 sind in folgenden Versionen von PAN-OS ausnutzbar:

- PAN-OS 11.2 vor Version 11.2.4-h1
- PAN-OS 11.1 vor Version 11.1.5-h1
- PAN-OS 11.0 vor Version 11.0.6-h1
- PAN-OS 10.2 vor Version 10.2.12-h2

Für PAN-OS-Versionen vor 10.1.14-h6 besteht außerdem eine Gefährdung durch CVE-2024-9474, nicht jedoch durch CVE-2024-0012. Cloud NGFW und Prisma Access sind jeweils von keiner der genannten Schwachstellen betroffen.

Bewertung

Firewalls stellen als zentrale Sicherheitslösung ein attraktives Angriffsziel dar, da sie den gesamten Netzwerkverkehr kontrollieren und schützen. Eine Kompromittierung ermöglicht es Angreifenden, Zugriff auf interne Netzwerke und damit sensible Daten und Dienste zu erhalten. Nicht hinreichend abgesicherte Management Interfaces bzw. administrative Zugänge dienen dabei oftmals als Einstieg und können in der Folge für weiterführende Angriffe (Lateral Movement) genutzt werden.

Trotz dieses grundsätzlichen Bedrohungsszenarios werden diese Einstiegspunkte von Administratoren in der Praxis häufig nicht ausreichend geschützt, sodass es in der Vergangenheit immer wieder zu erfolgreichen Angriffen auf Firewalls verschiedener Hersteller über administrative Zugänge gekommen ist.

Update 1:

In Deutschland sind nach einem Scan der Shadowserver Foundation weiterhin ca. 100 Systeme mit einem exponierten Palo Alto Management Interface im Internet zu finden [SHAD24] (Stand 18.11.2024).

Maßnahmen

IT-Sicherheitsverantwortliche sollten schnellstmöglich prüfen, ob eine der von ihnen verwalteten Firewalls das Management Interface zum Internet exponiert. Hierzu können einerseits die Ergebnisse des von Palo Alto durchgeführten Scans gesichtet, andererseits aber auch selbst die Konfigurationen der betriebenen Geräte eingesehen werden. Außerdem sollten die Schritte zur Absicherung des Management Zugriffs in der Anleitung [PALO24b] umgesetzt werden.

Cortex Xpanse- und Cortex XSIAM-Kunden mit dem ASM-Modul können außerdem öffentlich zugängliche Instanzen untersuchen, indem sie die von der Palo Alto Networks Firewall Admin Login-Angriffsflächenregel generierten Warnmeldungen überprüfen.

IT-Sicherheitsverantwortlichen wird weiterhin empfohlen, das Advisory [PALO24a] regelmäßig auf Aktualisierungen zu sichten und dazu den RSS-Feed oder die E-Mail Benachrichtigungen für Kunden zu abonnieren. Sobald in diesem Zusammenhang Patches verfügbar sind, sollten diese ebenfalls schnellstmöglich installiert werden.

Zum aktuellen Zeitpunkt liegen keine Indikatoren vor, die zur Identifizierung einer erfolgreichen Ausnutzung verwendet werden können. IT-Sicherheitsverantwortliche sollten daher auf generelle Auffälligkeiten – wie Konfigurationsänderungen sowie neue oder modifizierte Nutzer – achten.

Aufgrund der Tatsache, dass laut Hersteller bereits Angriffe stattgefunden haben, empfiehlt das BSI zusätzlich, die Zugangsdaten der Firewalls mit exponierten Management Interface zu erneuern, nachdem die Schritte zur Absicherung [PALO24b] durchgeführt wurden.

Das BSI empfiehlt IT-Sicherheitsverantwortlichen, die Vorgaben im Grundschutz (NET.3.2 Firewall) umzusetzen [BSI23]. Dort wird u.a. ausgeführt: *"Alle Administrations- und Managementzugänge der Firewall MÜSSEN auf einzelne Quell-IP-Adressen bzw. -Adressbereiche eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann."*.

Update 1:

Palo Alto Networks hat Patches veröffentlicht, um die zwei gefundenen Schwachstellen zu schließen. Die Versionen

- PAN-OS 11.2 Version 11.2.4-h1
- PAN-OS 11.1 Version 11.1.5-h1
- PAN-OS 11.0 Version 11.0.6-h1
- PAN-OS 10.2 Version 10.2.12-h2

schützen vor einer Ausnutzung. Für PAN-OS 10.1 schließt 10.1.14-h6 oder höher die für diese Version relevante Schwachstelle CVE-2024-9474.

Es stehen ebenso zusätzliche Patches für weitere Maintenance-Releases zur Verfügung. Mehr dazu im Advisory [PALO24a]. Dort finden sich ebenfalls Informationen, wie Kunden mit Threat Prevention Abonnement Angriffe mithilfe der Threat IDs 95746, 95747, 95752, 95753, 95759 und 95763 (verfügbar in Applications and Threats - Version 8915-9075 und neuer) blockieren können.

Der Hersteller hat außerdem Indikatoren für eine Kompromittierung herausgegeben [PALO24d]. Hierzu zählen einerseits IP-Adressen, die bei Scans und Angriffsversuchen beobachtet wurden, andererseits auch Payloads aus erfolgreichen Attacken. IT-Sicherheitsverantwortliche sollten auf Basis dieser Anhaltspunkte daher zusätzlich prüfen, ob verdächtige Aktivitäten in Log-Dateien nachgewiesen werden können.

Links

[PALO24a] PAN-SA-2024-0015 Critical Security Bulletin: Ensure Access to Management Interface is Secured
https://security.paloaltonetworks.com/PAN-SA-2024-0015

[PALO24b] How to Secure the Management Access of Your Palo Alto Networks Device:
https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431

[BSI23] BSI IT-Grundschutz-Baustein NET.3.2 Firewall (Edition 2023)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2023

Update 1:

[PALO24c] CVE-2024-9474 PAN-OS: Privilege Escalation (PE) Vulnerability in the Web Management Interface
https://security.paloaltonetworks.com/CVE-2024-9474

[PALO24d] Threat Brief: Operation Lunar Peek, Activity Related to CVE-2024-0012:
https://unit42.paloaltonetworks.com/cve-2024-0012-cve-2024-9474/

[SHAD24] Shadowserver Foundation - Palo Alto Networks Geräte mit exponierten Management Interface
https://dashboard.shadowserver.org/statistics/iot-devices/map/?

day=2024-11-18&vendor=palo+alto+networks&model=pan-os+management+interface&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.