２０２４年１０月１１日

お客様各位

株式会社日立ソリューションズ
Palo Alto Networks 製品ユーザーサポート

悪意のあるパケットによるサービス拒否(DoS)の脆弱性(CVE-2024-9468)について

平素は Palo Alto Networks 製品ユーザーサポートをご利用くださいまして誠にありがとうございます。この度、Palo Alto Networks 社より、悪意のあるパケットによるサービス拒否(DoS)の脆弱性(CVE-2024-9468)についてアナウンスされましたので、以下の通りご連絡いたします。

1. 概要

PAN-OS ソフトウェアのメモリ破損の脆弱性により、攻撃者がデータプレーンを介して細工されたパケットによって PAN-OS をクラッシュさせ、サービス拒否（DoS）状態を引き起こす可能性があります。サービス拒否（DoS）状態を複数回引き起こされると、PAN-OS がメンテナンスモードに入ります。

2. 対象のお客様

下記の表で影響を受けるバージョンをご利用されているお客様。

表 1 対象 OS バージョン

OS バージョン	影響を受ける	影響を受けない
Cloud NGFW	None	All
PAN-OS 11.2	None	All
PAN-OS 11.1	<11.1.3	≧11.1.3
PAN-OS 11.0	<11.0.4-h5、<11.0.6	≧11.0.4-h5、≧11.0.6
PAN-OS 10.2	<10.2.9-h11、 <10.2.10-h4、 <10.2.11	≧10.2.9-h11、 ≧10.2.10-h4、≧10.2.11
PAN-OS 10.1	None	All
Prisma Access	None	All

3. 本脆弱性に該当する構成

本脆弱性は以下のすべての条件に該当する PA シリーズが影響を受けます。

- Threat Prevention が有効になっている。
- Threat ID 86467（Name："Domain Fronting Detection-SNI"）が Anti-Spyware プロファイルで有効になっている。
- Domain Fronting Detection が有効になっている。（Device > Setup > Session > Decryption Settings > SSL Decryption Settings > Send handshake messages to CTD for inspection が有効になっている）

4. 回避策

Domain Fronting Detection を無効にすることで本脆弱性の悪用を防ぐことができます。（Device > Setup > Session > Decryption Settings > SSL Decryption Settings > Send handshake messages to CTD for inspection のチェックを外し無効にする）

Threat Prevention サブスクリプションをご契約のお客様で、Domain Fronting Detection をご利用する場合は、Threat ID 94971（Applications and Threats content version 8854 で導入）を有効にすることで本脆弱性に対する攻撃をブロックすることができます。

5. 恒久対策

下記 OS バージョンへのアップグレードをご検討ください。

表 2 修正に対応している OS バージョン

対象 OS バージョン	修正 OS バージョン
Cloud NGFW	All
PAN-OS 11.2	All
PAN-OS 11.1	≧11.1.3
PAN-OS 11.0	≧11.0.4-h5、≧11.0.6
PAN-OS 10.2	≧10.2.9-h11、≧10.2.10-h4、≧10.2.11
PAN-OS 10.1	All
Prisma Access	All

6. その他特記事項

本脆弱性の詳細や最新情報については、下記の Palo Alto Networks 社ページも併せてご参照ください。

CVE-2024-9468 PAN-OS: Firewall Denial of Service (DoS) via a Maliciously Crafted Packet
https://security.paloaltonetworks.com/CVE-2024-9468

なお、掲載されている以上の情報は開示されておりません。記載内容以上の情報については、弊社サポートではお答え致しかねますことを予めご了承ください。

また、Palo Alto Networks 社からは、2024 年 10 月 10 日に本脆弱性以外にも Palo Alto Networks 社製品に関するセキュリティアドバイザリーが複数発表されております。（Critical 1 件、High 2 件、Medium 4 件）
下記、 Security Advisories からご参照ください。

Security Advisories
https://security.paloaltonetworks.com

以上