

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

DNS セキュリティを利用したサービス拒否(DoS)の脆弱性(CVE-2024-3393)について (第2報)

平素は Palo Alto Networks 製品ユーザーサポートをご利用くださり誠にありがとうございます。この度、Palo Alto Networks 社より、DNS セキュリティを利用したサービス拒否 (DoS) の脆弱性 (CVE-2024-3393) 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。

※太字箇所は追記もしくは変更箇所となっております。

1. 概要

PAN-OS の DNS セキュリティ機能にサービス拒否 (DoS) の脆弱性があり、攻撃者が PAN-OS のデータプレーンを介して悪意のあるパケットを送信し、PAN-OS を再起動させることができます。この状態を繰り返し行うことで PAN-OS がメンテナンスモードになります。

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
Panorama	None	All
PAN-OS 11.2	11.2.3 未満	11.2.3 以上
PAN-OS 11.1	11.1.5 未満	11.1.5 以上
PAN-OS 10.2	10.2.8 以上、 10.2.14 未満	10.2.8 未満、 10.2.14 以上
PAN-OS 10.1	10.1.14 以上、 10.1.15 未満	10.1.14 未満、 10.1.15 以上
PAN-OS 10.0	None	All
PAN-OS 9.1	None	All
Prisma Access	10.2.8 以上、 11.2.3 未満	10.2.8 未満、 11.2.3 以上

3. 本脆弱性に該当する構成

本脆弱性は、DNS セキュリティライセンスまたは Advanced DNS セキュリティライセンスを適用している PA シリーズ (VM シリーズ含む) および Prisma Access において、DNS セキュリティログを有効にしている場合、影響を受けます。

※ Cloud NGFW、Panorama M-Series、Panorama 仮想アプライアンスは影響を受けません。

4. 脅威活動

Palo Alto Networks 社は、本脆弱性を引き起こす悪意のある DNS パケットを PAN-OS がブロックしたときに、サービス拒否 (DoS) が発生したお客様がいることを確認しています。

5. 回避策

影響を受ける PAN-OS にすぐに対策 OS バージョンを適用できない場合は、導入環境に応じて以下の回避策の実施をご検討ください。

対象製品 : PA シリーズ (VM シリーズ含む)、Panorama によって管理されている Prisma Access

(1). Objects → Security Profiles にて定義済みの Anti-spyware プロファイルを使用している場合は、それを複製してカスタム Anti-spyware プロファイルとしてセキュリティルール (Policies → Security → (セキュリティルールの) Actions → Profiles または Actions → Group) へ適用します。

(2). Objects → Security Profiles → Anti-spyware → 対象のプロファイルを選択 → DNS Policies → DNS Security へ移動します。

(3). プロファイルにて構成されているすべての DNS セキュリティカテゴリのログの重大度 (Log Severity) を「none」に変更します。

(4). コミットします。

※ 対策 OS バージョンを適用後は、ログの重大度 (Log Severity) 設定を元に戻してください。

6. 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。

※ PAN-OS 11.0 系は 2024 年 11 月 17 日にサポート終了 (EOL) となったため、本脆弱性の対策 OS バージョンのリリース予定はありません。

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
Panorama	All
PAN-OS 11.2	11.2.3 以上
PAN-OS 11.1	11.1.5 以上
PAN-OS 10.2	10.2.14 以上
PAN-OS 10.1	10.1.15 以上
PAN-OS 10.0	All
PAN-OS 9.1	All
Prisma Access	11.2.3 以上

本脆弱性の影響を受ける Prisma Access をご利用のお客様は、恒久対策が実施されるまで回避策の実施をご検討ください。恒久対策となる Prisma Access のアップグレードは、2025 年 1 月 3 日と 2025 年 1 月 10 日の週末に 2 段階に分けて実施されます。

また、追加で下記対策 OS バージョンもリリースされています。

- PAN-OS 11.1 の追加対策 OS バージョン
11.1.2-h16、11.1.3-h13、11.1.4-h7、11.1.5
- PAN-OS 10.2 の追加対策 OS バージョン
10.2.8-h19、10.2.9-h19、10.2.10-h12、10.2.11-h10、10.2.12-h4、
10.2.13-h2、10.2.14*1
- PAN-OS 10.1 の追加対策 OS バージョン
10.1.14-h8、10.1.15*1
- Prisma Access にのみ適用される追加対策 OS バージョン
10.2.9-h19、10.2.10-h12

*1 2025 年 1 月末リリース予定です。

7. 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-2024-3393 PAN-OS: Firewall Denial of Service (DoS) in DNS Security Using a Specially Crafted Packet

<https://security.paloaltonetworks.com/CVE-2024-3393>

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。

以上