２０２５年2月１４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

PAN-OS OpenConfig プラグインのコマンドインジェクション脆弱性(CVE-2025-0110)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、PAN-OS OpenConfig プラグインのコマンドインジェクション脆弱性(CVE-2025-0110)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

Palo Alto Networks PAN-OS OpenConfig プラグインのコマンドインジェクション脆弱性により、認証された管理者は PAN-OS 管理 Web インターフェイスに gNMI 要求を送信してシステム制限を回避し、任意のコマンドを実行できるようになります。コマンドは、PA シリーズ（VM シリーズ含む）上で「__openconfig」ユーザー（デバイス管理者の役割を持つ）として実行されます。

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 対象バージョン

バージョン	影響を受ける	影響を受けない
PAN-OS OpenConfig プラグイン	2.1.2 未満	2.1.2 以上

3. 本脆弱性に該当する構成

PAN-OS ソフトウェアは、OpenConfig プラグインを有効にした場合のみ本脆弱性の影響を受けます。

- OpenConfig プラグインバージョン 2.0.1 以降は、PAN-OS バージョン 11.0.4 およびそれ以降のすべての PAN-OS バージョンに自動的にインストールされます。
- OpenConfig プラグインバージョン 2.0.2 以降は、PAN-OS バージョン 10.2.11 以降の PAN-OS 10.2 バージョンに自動的にインストールされます。

OpenConfig プラグインは、ポート番号 9339 の PAN-OS 管理インターフェイス上の管理者がアクセス可能です。

使用している OpenConfig プラグインのバージョンを確認するには、次の手順に従ってください。

(1). Device > Plugin を選択

(2). 現在インストールされている OpenConfig プラグインのバージョンには、「CURRENTLY INSTALLED」にチェックマークが付いています。

4. 脅威活動

Palo Alto Networks 社は、本脆弱性を悪用した事例は認識しておりません。

5. 回避策

影響を受ける PA シリーズ（VM シリーズ含む）にすぐに恒久対策を実行出来ない場合は、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。

Palo Alto Networks 社のベストプラクティスの導入ガイドラインに従って管理インターフェイスへのアクセスを信頼できる内部 IP アドレスのみに制限する
ベストプラクティスの導入ガイドライン
https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431
ベストプラクティスに関する詳細なドキュメント
https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices

OpenConfig プラグインを使用しない場合は、次の手順に従って無効化またはアンインストールを実施してください。

(1). Device > Plugin を選択

(2). CURRENTLY INSTALLED の項目を確認し、インストールされている Open-Config プラグインを見つけます。

(3). Remove Config を選択して OpenConfig プラグインを無効化する、または Uninstall を選択して OpenConfig プラグインを削除します。

6. 恒久対策

本脆弱性は、PAN-OS OpenConfig プラグイン 2.1.2 およびそれ以降のすべての PAN-OS OpenConfig プラグインバージョンで修正されています。Panorama プラグインのアップグレードプロセスに従うことで、PAN-OS バージョンを更新せずに OpenConfig プラグインを更新できます。

OpenConfig プラグイン 2.1.2 は、PAN-OS 11.2.5 およびそれ以降のすべての PAN-OS バージョンに自動的にインストールされています。

Panorama プラグインのアップグレードプロセス
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-upgrade/upgrade-panorama-plugins/upgrade-a-panorama-plugin

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-2025-0110 PAN-OS OpenConfig Plugin: Command Injection Vulnerability in OpenConfig Plugin
https://security.paloaltonetworks.com/CVE-2025-0110
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、2025 年 2 月 13 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。（High 2 件、Medium 6 件、Informational 2 件）
これらについても上記の Security Advisories からご参照ください。

以上