２０２５年２月２１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 管理インターフェイスでの認証バイパス(CVE-2025-0108)を利用した攻撃の可能性（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 管理インターフェイスでの認証バイパス(CVE-2025-0108)を利用した攻撃の可能性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

Palo Alto Networks PAN-OS ソフトウェアの認証バイパスにより、PAN-OS 管理インターフェイスへのネットワークアクセス権を持つ攻撃者は、PAN-OS 管理インターフェイスで必要な認証を回避し、特定の PHP スクリプトを呼び出すことができます。これらの PHP スクリプトを呼び出してもリモートコード実行は行えませんが、PAN-OS の整合性と機密性に悪影響を与える可能性があります。

また、本脆弱性の公開に伴い、Palo Alto Net works 社は PAN-OS 管理インターフェイスへのアクセスが推奨されている設定の導入ガイドラインに従って正しく構成されていることを確認することを推奨しております。

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	11.2.4-h4 未満	11.2.4-h4 以上
PAN-OS 11.1	**11.1.2-h18 未満**、11.1.6-h1 未満	**11.1.2-h18 以上**、11.1.6-h1 以上
PAN-OS 10.2	**10.2.7-h24 未満、10.2.8-h21 未満、10.2.9-h21 未満、10.2.10-h14 未満 10.2.11-h12 未満、10.2.12-h6 未満**、10.2.13-h3 未満	**10.2.7-h24 以上、10.2.8-h21 以上、10.2.9-h21 以上、10.2.10-h14 以上 10.2.11-h12 以上、10.2.12-h6 以上**、10.2.13-h3 以上

PAN-OS 10.1	10.1.14-h9 未満	10.1.14-h9 以上
Prisma Access	None	All

3. 本脆弱性に該当する構成

インターネットまたは信頼できないネットワークから、管理ポート（MGT）もしくは DataPlane インターフェイス経由で PAN-OS 管理インターフェイスへのアクセスを有効にするようにデバイス設定が構成されている場合、本脆弱性に対するリスクが最大になります。

※ DataPlane インターフェイス経由で PAN-OS 管理インターフェイスへアクセスするには、PAN-OS 管理インターフェイスプロファイルの設定が必要です。

上記構成に該当するデバイスは、カスタマーサポートポータルの資産セクションの「Remediation Required」リストに表示されます。このリストを確認するには CSP アカウントを所有している必要があります。

※ 「Remediation Required」リストは完全ではない可能性があるため全てのデバイスで推奨設定を満たしていることを確認してください。

※ 検知方法に関する詳細につきましては弊社サポートサイトに掲載しているトピック「[重要]PAN-OS 管理インターフェイスの脆弱性を利用した攻撃の可能性」の最新報をご参照ください。

確認方法

(1). カスタマーサポートポータル（https://support.paloaltonetworks.com）の資産セクション（Products → Assets → All Assets → Remediation Required）にアクセスします。

(2). スキャンで検出された PAN-OS 管理インターフェイスを備えたデバイスのリストには、PAN-SA-2024-0015 のタグが付けられます。そのようなデバイスがリストにない場合は、スキャンにてインターネットに接続された PAN-OS 管理インターフェイスを備えたデバイスが検出されなかったことを意味します。

GlobalProtect ポータルと GlobalProtect ゲートウェイはこの問題の影響を受けません。ただし、GlobalProtect ポータルまたは GlobalProtect ゲートウェイとのインターフェイスで管理プロファイルを構成すると、PAN-OS 管理インターフェイス（通常はポート番号 4443 でアクセス可能）を介してデバイスが攻撃にさらされることになります。

4. 脅威活動

Palo Alto Networks 社は、対策 OS バージョンを適用しておらず、PAN-OS 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していない機器において CVE-2025-0108、CVE-2024-9474、および CVE-2025-0111 を利用した脅威活動を確認しました。

Privilege Escalation (PE) Vulnerability in the Web Management Interface
https://security.paloaltonetworks.com/CVE-2024-9474
Authentication Bypass in the Management Web Interface
https://security.paloaltonetworks.com/CVE-2025-0108
Authenticated File Read Vulnerability in the Management Web Interface
https://security.paloaltonetworks.com/CVE-2025-0111

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 PAN-OS 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

脅威防止サブスクリプションをお持ちのお客様は、Threat ID 510000 および 510001（Applications and Threats content version 8943 以降で利用可能）を有効にすることで、本脆弱性に対する攻撃をブロックできます。

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
PAN-OS 11.2	11.2.4-h4 以上
PAN-OS 11.1	**11.1.2-h18 以上**、11.1.6-h1 以上
PAN-OS 11.0	サポートされている修正済みバージョンへのアップグレード
PAN-OS 10.2	**10.2.7-h24 以上、10.2.8-h21 以上、10.2.9-h21 以上、10.2.10-h14 以上 10.2.11-h12 以上、10.2.12-h6 以上**、10.2.13-h3 以上
PAN-OS 10.1	10.1.14-h9 以上
Prisma Access	All

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。

Authentication Bypass in the Management Web Interface
https://security.paloaltonetworks.com/CVE-2025-0108
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。

脅威活動が確認されたことにより、下記アドバイザリの重要度が Medium から High に引き上げられています。こちらも併せてご参照ください。
Authenticated File Read Vulnerability in the Management Web Interface
https://security.paloaltonetworks.com/CVE-2025-0111

以上