２０２４年１１月２５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

[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（第 6 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の脆弱性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

PAN-OS 管理インターフェイスを介したリモートコード実行の脆弱性に関する情報が Palo Alto Networks 社より報告されました。本脆弱性の公開に伴い、Palo Alto Networks 社は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。
本脆弱性は当初、Severity が Information として公開されていましたが、Palo Alto Networks 社にて本脆弱性を悪用する兆候が確認されたことから、Critical に引き上げられました。

2. 対象のお客様

以下のいずれかにて PAN-OS 10.2、PAN-OS 11.0、PAN-OS 11.1、および PAN-OS 11.2 をご利用されているお客様。

(1). PA シリーズ（VM シリーズ含む）
(2). CN シリーズ
(3). Panorama（M シリーズ含む）
(4). WF-500 および WF-500-B WildFire アプライアンス

影響を受ける対象 OS バージョンの詳細につきましては下記の表をご参照ください。

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	11.2.0-h1 未満	11.2.0-h1 以上
	11.2.1-h1 未満	11.2.1-h1 以上

	11.2.2-h2 未満	11.2.2-h2 以上
	11.2.3-h3 未満	11.2.3-h3 以上
	11.2.4-h1 未満	11.2.4-h1 以上
PAN-OS 11.1	11.1.0-h4 未満	11.1.0-h4 以上
	11.1.1-h2 未満	11.1.1-h2 以上
	11.1.2-h15 未満	11.1.2-h15 以上
	11.1.3-h11 未満	11.1.3-h11 以上
	11.1.4-h7 未満	11.1.4-h7 以上
	11.1.5-h1 未満	11.1.5-h1 以上
PAN-OS 11.0	11.0.0-h4 未満	11.0.0-h4 以上
	11.0.1-h5 未満	11.0.1-h5 以上
	11.0.2-h5 未満	11.0.2-h5 以上
	11.0.3-h13 未満	11.0.3-h13 以上
	11.0.4-h6 未満	11.0.4-h6 以上
	11.0.5-h2 未満	11.0.5-h2 以上
	11.0.6-h1 未満	11.0.6-h1 以上
PAN-OS 10.2	10.2.0-h4 未満	10.2.0-h4 以上
	10.2.1-h3 未満	10.2.1-h3 以上
	10.2.2-h6 未満	10.2.2-h6 以上
	10.2.3-h14 未満	10.2.3-h14 以上
	10.2.4-h32 未満	10.2.4-h32 以上
	10.2.5-h9 未満	10.2.5-h9 以上
	10.2.6-h6 未満	10.2.6-h6 以上
	10.2.7-h18 未満	10.2.7-h18 以上
	10.2.8-h15 未満	10.2.8-h15 以上
	10.2.9-h16 未満	10.2.9-h16 以上
	10.2.10-h9 未満	10.2.10-h9 以上
	10.2.11-h6 未満	10.2.11-h6 以上
	10.2.12-h2 未満	10.2.12-h2 以上
PAN-OS 10.1	None	All
Prisma Access	None	All

※　表は 2024/11/19 時点のものです。最新情報につきましてはメーカの Security Advisories をご参照ください。

3. 影響を受ける構成

直接または、PAN-OS 管理インターフェイスプロファイルを含む DataPlane インターフェイス経由でのインターネットまたは信頼できないネットワークから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。

4. 回避策

Palo Alto Networks 社は、PAN-OS 管理インターフェイスへのアクセスはインターネットからではなく、信頼できる内部 IP からのみ可能であることを確認することを推奨しております。

脅威防止サブスクリプションをお持ちの場合は、Threat ID 95746、95747、95752、95753、95759、95763（Applications and Threats content version 8915-9075 以降で利用可能）を使用してこれらの攻撃をブロックできます。

Threat ID を使用して本脆弱性に対する攻撃から保護する方法

① リストされているすべての Threat ID がブロックモードに設定されていることを確認してください。
② 管理アクセス用に DataPlane インターフェイスで管理プロファイルを適用する等で、MGT ポートの着信トラフィックを DataPlane ポート経由でルーティングできるようにします。
③ 受信トラフィック管理の証明書を置き換えます。
④ PAN-OS 管理インターフェイスへの受信トラフィックを復号化してファイアウォールが検査できるようにします。
⑤ 管理サービスへの受信トラフィックに対する脅威防止を有効にします。

詳細な手順につきましては下記リンクをご参照ください。

Deploy Administrative Access Best Practices

https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices#id59206398-3dab-4b2f-9b4b-7ea500d036ba

推奨設定の導入ガイドラインの詳細につきましては下記リンクをご参照ください。

https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431

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 対策 OS バージョン

対象 OS バージョン	対策 OS バージョン
PAN-OS 11.2	11.2.0-h1、11.2.1-h1、11.2.2-h2、11.2.3-h3、11.2.4-h1 以降
PAN-OS 11.1	11.1.0-h4、11.1.1-h2、11.1.2-h15、11.1.3-h11、11.1.4-h7、11.1.5-h1 以降
PAN-OS 11.0	11.0.0-h4、11.0.1-h5、11.0.2-h5、11.0.3-h13、11.0.4-h6、11.0.5-h2、11.0.6-h1 以降
PAN-OS 10.2	10.2.0-h4、10.2.1-h3、10.2.2-h6、10.2.3-h14、10.2.4-h32、10.2.5-h9、10.2.6-h6、10.2.7-h18、10.2.8-h15、10.2.9-h16、10.2.10-h9、10.2.11-h6、10.2.12-h2 以降

※ 表は 2024/11/19 時点のものです。最新情報につきましてはメーカの Security Advisories をご参照ください。

6. よくある質問（FAQ）

Q1）脅威活動に関連する IoC はありますか？

最新情報については、Unit42 脅威概要（https://unit42.paloaltonetworks.com/cve-2024-0012-cve-2024-9474/）を参照してください。

Q2）Xpanse と XSIAM を使用して PAN-OS 管理インターフェイスを識別できますか？

ASM モジュールを備えた Cortex Xpanse および Cortex XSIAM をご利用のお客様は、Attack Surface Rules によって生成されたアラートを確認して、インターネットに公開されているインスタンスを調査できます。

Q3）PAN-OS 管理インターフェイスが推奨設定に従って導入されている場合、何かアクションを実行する必要がありますか？
恒久対策に記載している対策 OS バージョンへのアップグレードをご検討ください。

Q4）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があることをどのような方法で確認していますか？
Palo Alto Networks 社は、非侵入型インターネットスキャンを通じて、インターネットに公開されているお客様デバイスの PAN-OS 管理インターフェイスを検出します。この結果は、独自のインジケーターを使用して分析され、デバイス属性（モデルなど）を高い精度で特定します。検出された IP アドレスに基づいて、Palo Alto Networks 社は、IP アドレスとシリアル番号を社内記録と相互参照することで、インターネットに公開されているデバイスを特定のお客様に関連付けることができます。

過去数日間にこの方法で検出されたデバイスは、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。

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。

Q5）デバイス上で脅威活動の痕跡を探すことができる手段はありますか？
PAN-OS 管理インターフェイスがインターネットに公開されている場合は、見覚えのないデバイスの構成変更や疑わしいユーザーが居ないか等の脅威アクティビティがないか注意深く監視することをお勧めします。

Palo Alto Networks 社は、テレメトリデータとお客様からご提供いただいたテクニカルサポートファイル（TSF）をスキャンして脅威アクティビティの証拠を探し、それに応じてケースノートを更新しています。

Q6）デバイス上で脅威活動が確認された場合、どのような対応を取ることをお勧めしていますか？
デバイスをインターネットから切り離し、デバイスの拡張ファクトリーリセット（EFR）の実施がメーカから推奨されています。EFR の実施手順等の詳細確認、および実施をご希望のお客様は弊社サポートまでご連絡ください。

EFR を使用したデバイスを修復する方法については下記をご参照ください。
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CrO6CAK

Q7）GlobalProtect ポータルとゲートウェイは本脆弱性の影響を受けますか？
いいえ、GlobalProtect ポータルおよびゲートウェイ（通常は、ポート 443 でアクセス可能）は本脆弱性の影響を受けません。ただし、GlobalProtect ポータルまたはゲートウェイのインターフェイス（通常は、ポート 4443 でアクセス可能）に管理プロファイルが設定されている場合、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介したデバイスへの攻撃が可能となります。

7. その他特記事項
本脆弱性を利用して CVE-2024-9474 など他の脆弱性も利用可能となります。
CVE-2024-9474 については下記の Palo Alto Networks 社ページをご参照ください。
CVE-2024-9474 PAN-OS: Privilege Escalation (PE) Vulnerability in the Web Management Interface
https://security.paloaltonetworks.com/CVE-2024-9474

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-2024-0012 PAN-OS: Authentication Bypass in the Management Web Interface (PAN-SA-2024-0015)
https://security.paloaltonetworks.com/CVE-2024-0012

以上