２０２４年１１月１８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 3 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

   現時点では、Palo Alto Networks 社が推奨する設定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が保護されていないデバイスは、悪用のリスクが増大していると考えられます。

3. 恒久対策

   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。

   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

4. よくある質問（FAQ）

Q1）本脆弱性は悪用されましたか？

はい、Palo Alto Networks 社は、インターネットに公開されている一部デバイスの PAN-OS 管理インターフェイスに対して、本脆弱性を利用した脅威活動を確認しました。

Q2）侵害の兆候はありますか？

はい、Palo Alto Networks 社は、以下の IP アドレスからインターネットに公開されている PAN-OS 管理インターフェイスの IP アドレスとポート宛てへの脅威アクティビティを確認しました。

- **136.144.17.***
- **173.239.218.251**
- **216.73.162.***

***は 0～255 のいずれかの数字が入ります。**

これらの IP アドレスは、サードパーティの VPN である可能性があり、これらの IP アドレスから他の宛先への正当なユーザーアクティビティが発信されている可能性があります。

Checksum が、
3C5F9034C86CB1952AA5BB07B4F77CE7D8BB5CC9FE5C029A32C72ADC7E814668 の Web shell を確認しました。

Q3）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。

Q4）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？

現時点でこれ以上のアクションは必要ありません。

Q5）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。

5. 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。

PAN-SA-2024-0015 Important Informational Bulletin: Ensure Access to Management Interface is Secured
https://security.paloaltonetworks.com/PAN-SA-2024-0015

以上