２０２４年１１月１２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の脆弱性を利用した攻撃の可能性

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。

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 社へ報告されました。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。

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、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？

いいえ、悪用行為は確認されておりません。

Q2）侵害の兆候はありますか？

いいえ、侵害の兆候を示す十分な情報はありません。

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。

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