２０２１年8月２０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

Web インターフェースの OS コマンドインジェクションの脆弱性 (CVE-2021-3050)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、Web インターフェースに OS コマンドインジェクションの脆弱性がある事が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

特定の OS バージョンを使用している場合に、Web インターフェースに OS コマンドインジェクションが発生してしまう脆弱性が存在しております。
Web インターフェースにリモート認証された場合、任意のコマンドを実行されてしまう可能性があります。

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使用しているお客様。

OS バージョン	影響を受ける	影響を受けない
PAN-OS 9.0	9.0.10 ～ 9.0.14	≦9.0.15
PAN-OS 9.1	9.1.4 ～ 9.1.10	≦9.1.11
PAN-OS 10.0	10.0.0 ～ 10.0.7	≦10.0.8
PAN-OS 10.1	10.1.0 ～ 10.1.1	≦10.1.2

※Prisma Access と PAN-OS 8.1.x の OS バージョンをご使用の方は影響ございません。

3. 回避策

恒久対策を実施するまでの間、Web インターフェース宛のトラフィックに対して、コンテンツアップデートバージョン「8438」以降に含まれている Threat ID シグネチャ「91439」を有効化することで本脆弱性に対しての攻撃が遮断されます。
また、本脆弱性は PAN-OS の管理インターフェースを保護するためのベストプラクティスに従うことで軽減されます。
ネットワークセグメンテーションまたは管理アクセスに制限をかけることが推奨されております。

下記の Palo Alto Networks 社ページも併せてご参照ください。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

4. 恒久対策

PAN-OS 9.0.15 以降、9.1.11 以降、10.0.8 以降、10.1.2 以降へのバージョンアップをご検討ください。

5. その他特記事項

Palo Alto Networks 社からは、2021 年 8 月 11 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同時に複数発表されております。（High 1 件、Medium 4 件、Information 1 件）
詳しくは弊社サポートサイトのセキュリティアドバイザリーをご参照ください。

・弊社サポートサイトー[技術情報]ー[セキュリティアドバイザリー]
https://csps.hitachi-solutions.co.jp/paloalto/share/tech/tech_info.html#sa

以上