２０２６年１１月１３日

お客様各位

株式会社日立ソリューションズ
Palo Alto Networks 製品ユーザサポート

PAN-OS での機密情報漏洩の脆弱性（CVE-2026-0331）について

平素は Palo Alto Networks 製品ユーザ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 ソフトウェアでの機密情報漏洩の脆弱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

認証されていない攻撃者が、PAN-OS ソフトウェアにデータプレーンインターフェース宛て、またはそれを経由するトラフィックを送信することで、ファイアーウォールおよび通信セッションに関する機密情報を取得できる可能性があります。該当するお客様は、PAN-OS ソフトウェアのアップグレードをご検討ください。

2. 影響を受けるバージョンおよび対策バージョン

以下、表 1 の影響を受けるバージョンで稼働している PA シリーズ（VM シリーズを含む）、Prisma Access および Cloud NGFW が本脆弱性の影響を受けます。なお、Panorama は本脆弱性の影響を受けません。

表 1　対象および対策 PAN-OS バージョン

PAN-OS バージョン(※1)	影響を受けるバージョン	対策バージョン
PAN-OS 12.2 系	12.2.2～12.2.4-h2 未満	12.2.4-h2 以上
PAN-OS 12.1 系	12.1.8～12.1.10-h4 未満	12.1.10-h4 以上
	12.1.5～12.1.7-h12 未満	12.1.7-h12 または 12.1.10-h4 以上
	12.1.2～12.1.4-h14 未満	12.1.4-h14 または 12.1.10-h4 以上
PAN-OS 11.2 系	11.2.14～11.2.16-h2 未満	11.2.16-h2 以上
	11.2.11～11.2.13-h5 未満	11.2.13-h5 または 11.2.16-h2 以上
	11.2.8～11.2.10-h18 未満	11.2.10-h18 または 11.2.16-h2 以上
	11.2.5～11.2.7-h24 未満	11.2.7-h24 または 11.2.16-h2 以上
	11.2.0～11.2.4-h24 未満	11.2.4-h24 または 11.2.16-h2 以上
PAN-OS 11.1 系	11.1.14～11.1.16-h5 未満	11.1.16-h5 以上
	11.1.11～11.1.13-h17 未満	11.1.13-h17 または 11.1.16-h5 以上
	11.1.8～11.1.10-h37 未満	11.1.10-h37 または 11.1.16-h5 以上
	11.1.7～11.1.7-h13 未満	11.1.7-h13 または 11.1.16-h5 以上
	11.1.5～11.1.6-h41 未満	11.1.6-h41 または 11.1.16-h5 以上
	11.1.0～11.1.4-h39 未満	11.1.4-h39 または 11.1.16-h5 以上

PAN-OS 10.2 系	10.2.17～10.2.18-h14 未満 10.2.14～10.2.16-h13 未満 10.2.11～10.2.13-h28 未満 10.2.8～10.2.10-h43 未満 10.2.0～10.2.7-h40 未満	10.2.18-h14 以上 10.2.16-h13 または 10.2.18-h14 以上 10.2.13-h28 または 10.2.18-h14 以上 10.2.10-h43 または 10.2.18-h14 以上 10.2.7-h40 または 10.2.18-h14 以上
Prisma Access 12.1	12.1.10-h4 未満(※2)	12.1.10-h4 以上(※2)
Prisma Access 11.2	11.2.7-h24 未満(※2)	11.2.7-h24 以上(※2)
Prisma Access 10.2	10.2.10-h43 未満(※2)	10.2.10-h43 以上(※2)
Cloud NGFW	全バージョン(※2)	-(※2)

※1 サポート終了済みの PAN-OS バージョンをご利用の場合は、サポート対象の対策バージョンへの移行をご検討ください。

※2 Prisma Access および Cloud NGFW は、Palo Alto Networks 社により次回の定期メンテナンスで対策バージョンへのアップグレードが実施される予定です。

3. 解決策

対象のお客様は、表 1 に記載の対策バージョンへのアップグレードをご検討ください。

4. その他特記事項

本脆弱性の詳細や最新情報は、下記のセキュリティアドバイザリを参照ください。

https://security.paloaltonetworks.com/CVE-2026-0331

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は、弊社サポートではお答えいたしかねますことをあらかじめご了承ください。

以上