２０２６年5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 製品ユーザサポート

IKEv2 処理におけるリモートコード実行の脆弱性(CVE-2026-0263)についてのお知らせ

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 IKEv2 処理におけるリモートコード実行の脆弱性(CVE-2026-0263)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 ソフトウェアの IKEv2 処理を利用したバッファオーバーフローの脆弱性により、攻撃者がサービス拒否(DoS)状態を引き起こすことや、攻撃者が細工したネットワークトラフィックを送信して任意のコードを実行する可能性があります。

2. 対象のお客様と対策バージョン

対象は表 1 の影響を受ける OS バージョンおよび構成でご利用されているお客様です。なお、Panorama、Cloud NGFW および Prisma Access は当該脆弱性の影響を受けません。

表 1 対象 OS バージョン

OS バージョン	影響を受ける OS バージョン	対策 OS バージョン
PAN-OS 12.1 系	12.1.5～12.1.6	12.1.7※以上
	12.1.2～12.1.4-h*	12.1.4-h5 または 12.1.7※以上
PAN-OS 11.2 系	11.2.12 未満	11.2.12※以上
	11.2.8～11.2.10-h*	11.2.10-h6 または 11.2.12※以上
	11.2.5～11.2.7-h*	11.2.7-h13 または 11.2.12※以上
	11.2.0～11.2.4-h*	11.2.4-h17※または 11.2.12※以上
PAN-OS 11.1 系	11.1.15 未満	11.1.15※以上
	11.1.11～11.1.13-h*	11.1.13-h5 または 11.1.15※以上
	11.1.8～11.1.10-h*	11.1.10-h25 または 11.1.15※以上
	11.1.7～11.1.7-h*	11.1.7-h6※または 11.1.15※以上
	11.1.5～11.1.6-h*	11.1.6-h32 または 11.1.15※以上
	11.1.0～11.1.4-h*	11.1.4-h33 または 11.1.15※以上
PAN-OS 10.2	影響なし	全バージョン

※　5/28(米国時間)にメーカリリース予定。

当該事象の影響を受けるのは、以下の条件を満たしている構成です。

- NIST の承認を受けていない耐量子暗号(PQC)で構成された IKEv2 VPN トンネルを利用している場合。

3. 回避策および緩和策

IKEv2 VPN をご利用のお客様は、NIST が承認した耐量子暗号(PQC)のみを使用して IKEv2 VPN トンネルを設定することで、この問題を軽減できます。

4. 解決策

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

5. その他特記事項

本トピック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。

https://security.paloaltonetworks.com/CVE-2026-0263

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については、弊社サポートではお答え致しかねますことを予めご了承ください。

以上