２０２６年9月１４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 XML 処理によるバッファオーバーフローの脆弱性（CVE-2026-0310）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 での XML 処理によるバッファオーバーフローの脆弱性（CVE-2026-0310）がアナウンスされました。

1. 概要

PAN-OS の XML 処理機能にはバッファオーバーフローの脆弱性があります。本脆弱性を悪用された場合、管理インターフェイス（MGT）またはデータプレーンインターフェイスへのネットワークアクセス権を持つ攻撃者によって、PA シリーズ（VM シリーズ含む）および Panorama に対してサービス停止（DoS）や管理者権限で任意のコードが実行される可能性があります。該当するお客様におかれましては、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. 対象のお客様および対策バージョン

対象は表 1 の影響を受ける PAN-OS バージョンで稼働している PA シリーズ（VM シリーズ含む）および Panorama をご利用されているお客様です。なお、Cloud NGFW の全ての AWS および Azure 環境は当該脆弱性の影響を受けます。

表 1　対象 PAN-OS バージョン

PAN-OS バージョン	影響を受ける PAN-OS バージョン	対策 PAN-OS バージョン
PAN-OS 12.2 系	12.2.3 未満	12.2.3 以上
PAN-OS 12.1 系	12.1.10 未満 12.1.7-h5 未満 12.1.4-h10 未満	12.1.10 以上 12.1.7-h5 または 12.1.10 以上 12.1.4-h10 または 12.1.10 以上
PAN-OS 11.2 系	11.2.13-h2 未満 11.2.10-h14 未満 11.2.7-h20 未満 11.2.4-h21 未満	11.2.13-h2 以上 11.2.10-h14 以上 11.2.7-h20 以上 11.2.4-h21 以上

PAN-OS 11.1 系	11.1.16-h2 未満 11.1.13-h12 未満 11.1.10-h33 未満 11.1.7-h10 未満 11.1.6-h38 未満 11.1.4-h36 未満	11.1.16-h2 以上 11.1.13-h12 以上 11.1.10-h33 以上 11.1.7-h10 以上 11.1.6-h38 以上 11.1.4-h36 以上
PAN-OS 10.2 系	10.2.18-h10 未満 10.2.16-h10 未満 10.2.13-h24 未満 10.2.10-h40 未満 10.2.7-h37 未満	10.2.18-h10 以上 10.2.16-h10 以上 10.2.13-h24 以上 10.2.10-h40 以上 10.2.7-h37 以上
Prisma Access 12.1	12.1.7-h5 未満	12.1.7-h5 以上
Prisma Access 11.2	11.2.7-h20 未満	11.2.7-h20 以上
Prisma Access 10.2	10.2.10-h40 未満	10.2.10-h40 以上

※　Prisma Access および Cloud NGFW については、Palo Alto Networks 社により次回の定期メンテナンスにて対策 PAN-OS 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

影響を受ける PAN-OS バージョンで稼働している PA シリーズ（VM シリーズ含む）、Panorama をご利用されているお客様は、表 1 に記載している対策 PAN-OS バージョンへのアップグレードをご検討ください。なお、本脆弱性に対する回避策はございません。

4. 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-2026-0310

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