

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 管理インターフェースの認証済みリモートコード実行の脆弱性 (CVE-2026-0322) 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り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 管理インターフェースのリモートコード実行の脆弱性 (CVE-2026-0322) 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 ソフトウェアの管理インターフェースに、認証済みの攻撃者によって悪用される可能性のあるリモートコード実行の脆弱性が存在します。本脆弱性が悪用された場合、認証済みの攻撃者によって管理インターフェースへアクセス可能な環境下で、ルート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 をご利用のお客様です。

なお、Cloud NGFW および Prisma Access は、この脆弱性の影響を受けません。

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	12.2.4 未満	12.2.4 以上
PAN-OS 12.1 系	12.1.8～12.1.10-h2 未満 12.1.5～12.1.7-h8 未満 12.1.2～12.1.4-h12 未満	12.1.10-h2 以上 12.1.7-h8 または 12.1.10-h2 以上 12.1.4-h12 または 12.1.10-h2 以上
PAN-OS 11.2 系	11.2.14～11.2.16 未満 11.2.11～11.2.13-h3 未満 11.2.8～11.2.10-h15 未満 11.2.5～11.2.7-h21 未満 11.2.0～11.2.4-h22 未満	11.2.16 以上 11.2.13-h3 または 11.2.16 以上 11.2.10-h15 または 11.2.16 以上 11.2.7-h21 または 11.2.16 以上 11.2.4-h22 または 11.2.16 以上
PAN-OS 11.1 系	11.1.14～11.1.16-h3 未満 11.1.11～11.1.13-h15 未満 11.1.8～11.1.10-h35 未満 11.1.7～11.1.7-h11 未満 11.1.5～11.1.6-h39 未満 11.1.0～11.1.4-h37 未満	11.1.16-h3 以上 11.1.13-h15 または 11.1.16-h3 以上 11.1.10-h35 または 11.1.16-h3 以上 11.1.7-h11 または 11.1.16-h3 以上 11.1.6-h39 または 11.1.16-h3 以上 11.1.4-h37 または 11.1.16-h3 以上

PAN-OS 10.2 系	10.2.17～10.2.18-h12 未満	10.2.18-h12 以上
	10.2.14～10.2.16-h11 未満	10.2.16-h11 または 10.2.18-h12 以上
	10.2.11～10.2.13-h26 未満	10.2.13-h26 または 10.2.18-h12 以上
	10.2.8～10.2.10-h41 未満	10.2.10-h41 または 10.2.18-h12 以上
	10.2.0～10.2.7-h38 未満	10.2.7-h38 または 10.2.18-h12 以上

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

3. 解決策

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

4. 緩和策

本脆弱性に対する既知の回避策はありませんが、Palo Alto Networks 社推奨のセキュリティのベストプラクティス(※1)を実施することで、本脆弱性のリスクを大幅に軽減できます。

また、脅威防御サブスクリプションをご利用のお客様は、脅威 ID 510046 および 510047（アプリケーションおよび脅威コンテンツバージョン 9159-10287 以降）を有効にし、SSL 復号化を含む管理アクセスのベストプラクティス(※2)を適用することで、本脆弱性に対する限定的な保護を受けることができます。

(※1) Critical Recommendations for Deployment Guides: How to Secure the Management Access to your Palo Alto Networks Device

<https://live.paloaltonetworks.com/t5/community-blogs/critical-recommendations-for-deployment-guides-how-to-secure-the/ba-p/464431>

(※2) Administrative Access Best Practices

<https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices#idbbd82587-17a2-42b4-9245-d3714e1e13a2>

5. その他特記事項

本トピック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ご参照ください。

<https://security.paloaltonetworks.com/CVE-2026-0322>

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