

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

PHP の脆弱性（CVE-2026-109618、CVE-2026-109619）の Palo Alto Networks 製品への影響

平素は Palo Alto Networks 製品ユーザサポートをご利用くださいますようお願いいたします。
この度、Palo Alto Networks 社より PHP に存在する重大な脆弱性（CVE-2026-109618、CVE-2026-109619）による同社製品への影響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

PHP において、リモートから任意コード実行が可能となる重大な脆弱性が報告されています。

CVE-2026-109618 は、メモリ不足発生時の `longjmp()` によるエラー処理の不備により、未初期化メモリを利用して任意コード実行が可能となる脆弱性です。

CVE-2026-109619 は、`longjmp()` による致命的エラー処理の不備により、解放済みメモリ領域への参照が残存し、その後のリクエストで任意コード実行が可能となる脆弱性です。

Palo Alto Networks 社より、PA シリーズ（VM シリーズを含む）および Panorama が本脆弱性の影響を受けることが確認されています。該当するお客様は、対策 PAN-OS バージョンのリリース後、アップグレードをご検討ください。また、リスク低減のため、脅威防御サブスクリプションの適用および管理アクセスのベストプラクティスの適用をご検討ください。

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 シリーズを含む）および Panorama をご利用のお客様です。

また、Bridgecrew、Cloud NGFW、Cortex XDR Agent、Cortex XSIAM、Cortex XSOAR、Cortex Xpanse、GlobalProtect App、Idira、Prisma Cloud、Prisma Access、Prisma Access Agent 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※1	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	全バージョン	提供時期未定※2
PAN-OS 12.1 系	全バージョン	提供時期未定※2
PAN-OS 11.2 系	全バージョン	提供時期未定※2
PAN-OS 11.1 系	全バージョン	提供時期未定※2
PAN-OS 10.2 系	全バージョン	提供時期未定※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 PAN-OS バージョンへの移行をご検討ください。

※2 対策 PAN-OS バージョンのリリース予定を含む最新情報は、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-2026-109618>

3. 解決策

対象のお客様は、今後リリースが予定されている表 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

Palo Alto Networks 社推奨のセキュリティのベストプラクティス※3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 543004、97622、97623、97624 および 97625（アプリケーションおよび脅威コンテンツバージョン 9162 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※4を適用することで、本脆弱性に対する保護を受けることができます。

※3 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>

※4 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#id59206398-3dab-4b2f-9b4b-7ea500d036ba>

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-2026-109618>

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