

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  
（第2報）

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**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。

※ 太字箇所は追記もしくは変更箇所となっております。

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（CVE-2026-109618、CVE-2026-109619）**が報告されています。また、Palo Alto Networks 社より、PA シリーズ（VM シリーズを含む）および Panorama などの製品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の影響を受けるバージョンで稼働している製品をご利用のお客様です。

表1 対象製品および対策バージョン

| 対象製品※1              |               | 影響を受けるバージョン    | 対策バージョン        | リリース予定日※3  |
|---------------------|---------------|----------------|----------------|------------|
| PA シリーズ（VM シリーズを含む） | PAN-OS 12.2 系 | 12.2.4-h1 未満   | 12.2.4-h1 以上   | 2026/10/28 |
|                     |               | 12.1.10-h3 未満  | 12.1.10-h3 以上  | 2026/10/30 |
|                     |               | 12.1.7-h11 未満  | 12.1.7-h11 以上  | 2026/10/28 |
|                     | PAN-OS 12.1 系 | 12.1.4-h13 未満  | 12.1.4-h13 以上  | 2026/10/29 |
|                     |               | 11.2.16-h1 未満  | 11.2.16-h1 以上  | 2026/10/28 |
|                     |               | 11.2.13-h4 未満  | 11.2.13-h4 以上  | 2026/10/27 |
|                     |               | 11.2.10-h16 未満 | 11.2.10-h16 以上 | 2026/10/26 |
|                     |               | 11.2.7-h23 未満  | 11.2.7-h23 以上  | 2026/10/29 |
|                     |               | 11.2.4-h23 未満  | 11.2.4-h23 以上  | 2026/10/30 |
|                     | PAN-OS 11.2 系 | 11.1.16-h4 未満  | 11.1.16-h4 以上  | 2026/10/26 |
|                     |               | 11.1.13-h16 未満 | 11.1.13-h16 以上 | 2026/10/27 |
|                     |               | 11.1.10-h36 未満 | 11.1.10-h36 以上 | 2026/10/28 |
|                     | PAN-OS 11.1 系 |                |                |            |

|  |                           |                |                |            |
|--|---------------------------|----------------|----------------|------------|
|  |                           | 11.1.7-h12 未満  | 11.1.7-h12 以上  | 2026/10/30 |
|  |                           | 11.1.6-h40 未満  | 11.1.6-h40 以上  | 2026/10/29 |
|  |                           | 11.1.4-h38 未満  | 11.1.4-h38 以上  | 2026/10/29 |
|  | PAN-OS 10.2 系             | 10.2.18-h13 未満 | 10.2.18-h13 以上 | 2026/10/26 |
|  |                           | 10.2.16-h12 未満 | 10.2.16-h12 以上 | 2026/10/28 |
|  |                           | 10.2.13-h27 未満 | 10.2.13-h27 以上 | 2026/10/27 |
|  |                           | 10.2.10-h42 未満 | 10.2.10-h42 以上 | 2026/10/29 |
|  |                           | 10.2.7-h39 未満  | 10.2.7-h39 以上  | 2026/10/30 |
|  | <b>Panorama</b>           |                | 全バージョン         | 未定※2       |
|  | <b>WF-500 及び WF-500-B</b> |                | 全バージョン         | 未定※2       |

※1 サポート終了済みの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 対策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 日付は米国時間を基準にしています。

なお、以下の製品は本脆弱性の影響を受けません。

Cloud NGFW、Prisma Access、Prisma Access Agent、GlobalProtect App、**WildFire Cloud**、**Strata Cloud Manager**、Prisma Cloud、Cortex XDR Agent、**Cortex XDR Broker VM**、**Cortex XCORE(SaaS)**、Cortex XSIAM、Cortex XSOAR、Cortex Xpanse、Bridgecrew、Idira

※ **Cortex XCORE(SaaS)**および **WildFire Cloud** は以前まで本脆弱性の影響を受けていましたが、それぞれ 2026 年 10 月 21 日あるいは 22 日(米国時間)に対策済です。

### 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※4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※5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。

※4 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>

※5 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