

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3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 (**M シリーズを含む**) 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。

2. 影響を受ける機能

管理用 Web インタフェース(WebUI、XML API サービス含む)が本脆弱性の影響を受けます。

3. 影響を受けるバージョンおよび対策バージョン

以下、表 1 の影響を受ける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 (M シリーズを含む)** が本脆弱性の影響を受けます。

※ 第2報では WF-500 及び WF-500B が対象と記載しておりましたが、その後の Palo Alto Networks 社アドバイザリの更新(影響なしに変更)に合わせ、掲載を外しています。

※ WildFire Cloud は本脆弱性の影響を受けていましたが、2026 年 10 月 23 日時点で対策済です。

表 1 対象および対策 PAN-OS バージョン

PAN-OS バージョン※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※2
PAN-OS 12.2 系	12.2.4-h1 未満	12.2.4-h1 以上	2026/10/28
PAN-OS 12.1 系	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
	12.1.4-h13 未満	12.1.4-h13 以上	2026/10/29

PAN-OS 11.2 系	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	リリース済
	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 11.1 系	11.1.16-h4 未満	11.1.16-h4	リリース済
	11.1.13-h16 未満	11.1.13-h16	リリース済
	11.1.10-h36 未満	11.1.10-h36	リリース済
	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	リリース済
	11.1.4-h38 未満	11.1.4-h38	リリース済
PAN-OS 10.2 系	10.2.18-h13 未満	10.2.18-h13	リリース済
	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

※1 PAN-OS 10.1 系未満の OS はサポート終了済みの為、本アナウンスの対象に含まれていません。

本表の対策バージョンへの移行をご検討ください。

※2 日付は米国時間を基準にしています。

4. 解決策

対象のお客様は、表 1 対策バージョンへのアップグレードをご検討ください。

5. 緩和策

Palo Alto Networks 社からはワークアラウンド/緩和策として、Threat Prevention を利用した方法がアナウンスされています。尚、本緩和策には別途設定が必要になる場合があります。

詳細は、同社セキュリティアドバイザリを参照ください。

※セキュリティアドバイザリには **Frontier Virtual Patching (ATP Plus)** を利用した方法も記載されていますが、同機能は本日（2026 年 10 月 26 日）時点でリリースされておりません。

6. 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