2026 年 10 月 29 日

お客様各位

株式会社日立ソリューションズ
Aruba Networks 製品ユーザーサポート

【脆弱性】PHP の脆弱性（CVE-2026-109618／CVE-2026-109619）の影響について（第 3 報）

平素は Aruba Networking 製品をご利用くださいまして誠にありがとうございます。

2026 年 10 月 21 日に報告された PHP の脆弱性（CVE-2026-109618／CVE-2026-109619）に関して、**2026 年 10 月 29 日 時点**で判明している当サポート対応製品における影響範囲、および解決策・回避策を以下にご案内します。

※ 太字箇所は追記もしくは変更箇所となっております。

敬具

記

1. CVE-2026-109618／CVE-2026-109619 の影響

現時点での影響確認状況は以下の通りです。

以下、影響を受ける製品に記載されていない製品およびバージョンは今回の脆弱性の影響を受けないと判断されています。

影響を受ける製品

- ClearPass　6.14.0 以前、6.11.15 以前(*1)

(*1) 4. 緩和策の通り、6.11.16 は対策バージョンではありません。
対策には 2 .対策バージョンに記載する Hotfix Patch を適用する必要があります。

2. 対策バージョン

ClearPass 6.14.1 および ClearPass 6.11.16 の Hotfix Patch により対策できます。

ClearPass 6.14.1 - CPHF 197　(*2)
ClearPass 6.11.16 - CPHF 196

(*2) 6.14.1 は弊社未リリース。

3. ワークアラウンド

ワークアラウンドとして、CLI および Web 管理インターフェースを専用の L2 セグメントに限定、又はファイアウォールで制御することが報告されています。

また、追加でユーザーの操作やリソース使用状況を追跡・記録すること、対策が完了するまで、ゲストポータル含む全ての管理インターフェースを、外部からアクセスできない状態にすることを検討する旨記載されています。

4. 緩和策

以下バージョンを利用することで、部分的に緩和されます。

- ClearPass 6.14.1 又は 6.11.16(*3)

(*3) 6.14.1 は弊社未リリース。

このバージョンを利用することで、影響を受ける条件が「認証不要」から、「クラスタ管理者権限（cluster-admin）で認証した場合」へ変わり、リスクが軽減されます。

5. メーカ情報

本情報は、以下でアナウンス更新されています。

詳細は、以下のメーカドキュメント(Web)を参照下さい。

HPESBNW05171 rev.1 - Multiple “PHP2Shell” Vulnerabilities identified in PHP allow for Unauthenticated Remote Code Execution in HPE Networking ClearPass Policy Manager

<https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05171en_us&docLocale=en_US>

6. 弊社更新について

弊社においても公開情報を継続して確認し、適宜更新いたします。

以上