FutureVuls

PHP重大脆弱性（通称 php2shell）2026年10月23日時点の事実整理

“今夜パッチを”の次に問われるのは“どこにPHPがあるか”

CVE-2026-109618 ／ CVE-2026-109619 ｜ 出典：PHP公式・JPCERT/CC・JVN・IPA・国家サイバー統括室

まず押さえる3つの事実

9.2

CVSS v4.0（2件とも）

PHP本体の脆弱性2件。認証もユーザー操作も不要で、リモートコード実行につながるおそれがあります。

4系列

修正版（10月21日公開）

8.5.12／8.4.27／8.3.36／8.2.35。サポート終了の8.1以前には公式の修正リリースがありません。

更新のみ

PHP公式の見解

「完全な緩和策はなく、更新が唯一の安全な選択肢」。設定変更は一部の経路を塞ぐだけです。

影響と修正版

系列	修正版	補足
PHP 8.5	**8.5.12**	セキュリティ修正〜2029年末
PHP 8.4	**8.4.27**	セキュリティ修正〜2028年末
PHP 8.3	**8.3.36**	セキュリティ修正〜2027年末
PHP 8.2	**8.2.35**	セキュリティ修正〜2026年末 終了間近のため移行計画も
8.1以前	**公式修正なし**	ディストリやLTSベンダーのバックポートを確認、またはサポート版へ移行

構成別のリスクと現在地

Apache mod_php は公式が「リスク最高」と明言

PHP-FPMやphp-cgiなど、Webリクエストを処理する構成はすべて対象です。

アップロード機能がないサイトも対象になりうる

PHPはアプリより前にリクエストを解析するため、アプリ側の対策だけでは防げません。

攻撃の試みは大量、侵害の成功は未確認

試行は数百万件規模で観測。侵害成功の公的確認はなく、CISA KEVも未掲載（10/23時点）。最新は一次情報で確認を。

今すぐ確認すべき8項目

緊急パッチを当てたあとに、改めて見直したい項目です

- [ ] **PHPを使うシステムの棚卸し**
  公開Webだけでなく、社内業務システム・CMS・パッケージ製品・アプライアンス内部のPHPも対象に。
- [ ] **ディストリ版は修正パッケージの有無を確認**
  バックポートではバージョン番号が変わらないことがあります。ベンダーのアドバイザリで確認を。
- [ ] **8.1以前は、移行・隔離・一時停止・公開終了を判断**
  IPAは公開終了やシステム廃止の検討も求めています。移行計画と暫定措置を分けて決めます。
- [ ] **WAFは補助策として位置づける**
  ルールの有効化は推奨ですが、回避を狙った攻撃の変化も報告されています。更新の代替にはしません。
- [ ] **実際に動いているバージョンの確認**
  php -v だけでなく、Webサーバ側で実際に使われているPHPを確認。CLIとWebで異なることがあります。
- [ ] **適用後にPHP-FPM／Apacheを再起動**
  再起動して反映されたことまで確認。更新しただけでは古いプロセスが残ります。
- [ ] **暫定策は「更新の代わりにならない」と共有**
  session.upload_progress の無効化などは一部の経路を塞ぐだけ。関係者の認識を揃えます。
- [ ] **侵害の痕跡を点検**
  異常なPHPSESSID Cookie・不審なmultipart・メモリ上限エラーをログで確認。調査は公表前（10/17ごろ）までさかのぼります。

出典：PHP公式勧告（php.net）／JPCERT/CC注意喚起 JPCERT-AT-2026-0033（2026/10/22）／JVNVU#99905564／
IPA注意喚起（2026/10/21・22）／国家サイバー統括室（X: @cyber_forecast）。
本資料は2026年10月23日時点の公開情報をもとにフューチャー株式会社が作成しました。最新情報は一次情報をご確認ください。

FutureVuls
https://www.vuls.biz
フューチャー株式会社
Cyber Security Innovation Group

本チラシ表面は、PHP脆弱性の公開情報を整理した参考資料です。
各システムへの適用可否は、必ずご自身の環境と一次情報でご確認ください。

次の“緊急パッチの夜”に備える

“PHPはどこにある？”に、すぐ答えられる組織へ

緊急の脆弱性が出るたびに「どのサーバで、どのバージョンが動いているか」を一から調べない運用へ。
FutureVulsは、資産と脆弱性と対応状況を一元管理するクラウド型の脆弱性管理サービスです。

よくあるお悩み

台帳が実態と合わない

Excelの台帳と、実際に動いているバージョンが一致しない。

優先順位がつけられない

重大と表示される脆弱性が多すぎて、今夜やるべきものが絞れない。

対応状況を追えない

誰がどのサーバまで対応したか、全社の状況が分からない。

FutureVuls なら

把握する

OS（Linux/Windows）、ミドルウェア、ライブラリ、コンテナ、NW機器、SBOMを一元管理。パッケージ管理外のソフトもCPEで登録。

判断する

SSVCで対応レベルを4段階に自動判定。KEV・PoCの有無やEPSSで「本当に今夜やるべきもの」を絞り込み。

追跡する

脆弱性ごと・サーバごとのタスク管理。アップデートコマンドの提示とコメントで、対応状況を全社で共有。

今回のような緊急脆弱性が出たとき

対応期限が“日”ではなく“時間”で語られる状況では、平時からの資産把握が前提になります。
該当するCVEがどのサーバ・どのグループにあるかを画面で横断確認し、対応タスクとして担当者に割り当てられます。完了状況はダッシュボードで可視化でき、経営層への報告にも活用できます。

製品にPHPを組み込むメーカーの方へ

出荷製品のSBOM管理と、自社製品向けの脆弱性のハンドリングには「PSIRTプラン」をご用意しています。

導入実績

金融・製造・通信など、大規模組織を中心に多くの企業でご利用いただいております。
導入事例は製品サイトでご覧いただけます。

資料ダウンロード

FutureVuls概要資料を
スマートフォンからご覧いただけます。

詳細・お問い合わせ

製品サイトから、機能の詳細や
導入事例をご確認ください。
https://www.vuls.biz

FutureVulsは脆弱性の把握と対応の管理を支援するサービスです。
記載内容は2026年10月23日時点のものです。