TLP:CLEAR【全分野】

別紙

2026 年 11 月 20 日

内閣官房　国家サイバー統括室
対処調整・官民連携等ユニット

PHP の深刻な脆弱性(CVE-2026-115560 等)について(注意喚起)

1. 対象ソフトウェア

PHP の次のバージョンが本脆弱性（CVE-2026-115560 等）の影響を受けます。

- PHP 8.5.13 未満
- PHP 8.4.28 未満
- PHP 8.3.37 未満
- PHP 8.2.36 未満

なお、PHP 8.1 以前はサポート対象外となるため、サポートされているバージョンへのアップグレードを推奨します。ただし、ディストリビューションや LTS ベンダーが独自にセキュリティ対応を実施している場合もあるため、利用している製品・サービスの提供元が提供する情報も併せて確認してください。

また、ファイアウォール、VPN ゲートウェイ、ロードバランサ、NAS、認証ゲートウェイ等のネットワーク機器やアプライアンス製品においても、管理画面等で PHP が内包されている可能性があります。各製品の開発元が提供する情報を確認してください。

2. 脆弱性悪用による影響等

今回、PHP によって修正されたセキュリティアップデートの中には、認証されていない第三者によってリモートコード実行につながる可能性のある脆弱性が含まれます。

例として、CVE-2026-115560 は、PHP のセッション処理における信頼できないデータのデシリアライゼーションに起因するリモートコード実行に関する脆弱性です。ただし、当該脆弱性は、サーバー起動時のセッションシリアライザを非標準形式に設定した上で、アプリケーション実行時にレガシー形式へ動的に切り替える構成など、特殊な条件が揃った場合にのみ成立します。詳細な条件については参考 URL①を参照してください。

なお、今回のセキュリティアップデートには、CVE-2026-115560 に加え、セッションファイルの不完全な書き込みによるデシリアライゼーションに起因するリモートコード実行（CVE-2026-126714）や、PHP-FPM のリクエストスマグリング（CVE-2026-129289）など、システムの完全掌握につながる複数の重大な脆弱性の修正が包括されています。

また、攻撃の成立条件は、各脆弱性によって異なるため、詳細な条件については脆弱性ごとのセキュリティアドバイザリを参照してください。

3. 悪用状況

本脆弱性について、現時点で悪用の観測は確認されていません。

4. 対応

開発元より、本脆弱性に対応するセキュリティアップデートおよび関連情報が公開されています。対象ソフトウェアを利用している組織は、開発元が案内する修正済みバージョンへのアップデートを実施するとともに、アクセスログ等で不審なセッション操作やリクエストの有無を確認することを推奨します（参考 URL①）。

5. 緩和策

開発元より、即時のアップグレードが困難な場合の暫定的な緩和策が脆弱性ごとに、公表されています。これらの対策はリスクを軽減するものであり、根本的な解決には修正済みバージョンへのアップグレードが必要です（参考 URL①）。適用時は、必ず事前検証し、業務要件との整合性を確認したうえで、適用を判断してください。例として、CVE-2026-115560 は、次の緩和策が案内されています。他の脆弱性については該当するセキュリティアドバイザリより緩和策をご確認ください。

＜セッションアップロード進捗機能の無効化＞

PHP の設定ファイル（php.ini）や PHP-FPM のプール設定（www.conf）において、以下のディレクティブを設定します。

```
session.upload_progress.enabled = 0
```

なお、設定変更後は、Web サーバーや PHP サービスを再起動し、設定が反映されていることを確認してください。

参考 URL

① PHP Project ChangeLog:
https://www.php.net/ChangeLog-8.php#8.5.13
https://www.php.net/ChangeLog-8.php#8.4.28
https://www.php.net/ChangeLog-8.php#8.3.37
https://www.php.net/ChangeLog-8.php#8.2.36