オムロン ロボティクス セキュリティ情報

PHP の脆弱性（PHP2Shell）- CVE-2026-109618 および CVE-2026-109619

1. 概要

オムロン ロボティクスは、広く使用されているオープンソースのサーバーサイドスクリプト言語である PHP で最近公開された、CVE-2026-109618 および CVE-2026-109619 として追跡され、総称して「PHP2Shell」と呼ばれる重大な脆弱性を認識しています。悪用に成功した場合、認証されていないリモート攻撃者が、影響を受ける PHP バージョンを実行しているシステム上で任意のコードを実行できる可能性があります。

当社の製品セキュリティインシデント対応チーム（PSIRT）は、組込み Web サーバー、設定インターフェース、および PHP をバンドルしている可能性のあるソフトウェアコンポーネントを含め、オムロン ロボティクス製品への影響を積極的に評価しています。本情報は、調査が完了するまで定期的に更新されます。

その間、お客様は、本情報に記載されたサイバーセキュリティのベストプラクティスおよび緩和策が、運用全体にわたって適用されていることを直ちに確認してください。

2. 脆弱性の詳細

2026 年 10 月 21 日、PHP プロジェクトは、PHP ランタイムに存在する 2 件の重大な脆弱性に対処するセキュリティアップデートを公開した。PHP-FPM、mod_php を使用する Apache、php-cgi、FrankenPHP、LiteSpeed を含め、Web リクエストを処理するすべての PHP インストール環境が潜在的なリスクにさらされている。実証済みのエクスプロイトでは、認証を要しない単一のリクエストによって、アプリケーションコードが実行される前に攻撃を誘発できることが示されている。公開された概念実証（PoC）が出回り始めている。

CVE ID	CVSS v4.0	説明
CVE-2026-109618 GHSA-w8hw-w9fx-j79w	9.2 Critical	メモリ不足（OOM）処理中のメモリ破損。リクエストが memory_limit を超過した場合、内部リクエストデータ（例：multipart 形式のファイルアップロード）が部分的にしか初期化されていない段階で、PHP が中断される可能性があります。その後のリクエストのクリーンアップ処理により、初期化されておらず、攻撃者が制御可能なデータを含む可能性があるメモリが解放され、リモートコード実行につながるおそれがあります。
CVE-2026-109619 GHSA-6wmf-4rv5-p3rp	9.2 Critical	古いグローバル状態の使用。リクエストに固有の内部状態が、そのバックアップメモリの解放後（致命的なエラー発生後など）にも存続する可能性があります。同じワーカーで後から処理されるリクエストが、通常の初期化によってリセットされる前にその古い状態を使用する可能性があり、リモートコード実行につながるおそれがあります。

影響を受ける PHP バージョン

- PHP 8.5.12 未満の PHP 8.5
- PHP 8.4.27 未満の PHP 8.4
- PHP 8.3.36 未満の PHP 8.3
- PHP 8.2.35 未満の PHP 8.2
- PHP プロジェクトから更新が提供されなくなった、サポート終了済みブランチ（PHP 8.1 以前）

注記：2026 年 10 月 23 日、PHP は、異例の構成を持つ Web アプリケーションにのみ影響する追加の RCE 脆弱性 CVE-2026-115560 を公開しました。これは本情報の対象外です。オムロン ロボティクスは本件を監視しており、該当する場合は今後の更新で対処します。

3. 影響を受ける製品、修正措置および緩和策

本書の公開日時点で、オムロン ロボティクスは以下の製品を評価中です。調査の進展に伴い、各製品のステータスは「影響あり」、「影響なし」または「修正済み」に更新されます。*

製品	バージョン	共通脆弱性識別子（CVE）	ステータス	修正／緩和策
SetNetGo（SNG）	SNG 7.x - PHP 5.6.24-0 SNG 8.x - PHP 8.1.22 SNG 9.x - PHP 8.2.34	CVE-2026-109618 CVE-2026-109619	**影響あり**	SNG 8.x および 9.x 向けのパッチが提供される予定です。パッチが適用されるまで、以下の推奨される緩和策を実施してください。 SNG 7.x では、以下の推奨される緩和策を実施するか、利用可能になり次第、パッチ適用済みの SNG 8.x または 9.x を含むサポート対象バージョンの FLOW へアップグレードする必要があります。
Fleet Operations Workspace（FLOW）Core／Fleet Manager	全バージョン(確認中)	CVE-2026-109618 CVE-2026-109619	**影響あり**	現在、評価中です。製品固有の情報が公開されるまで、以下の推奨される緩和策を適用してください。
モバイルロボット：LD シリーズ（LD-60/90/250）、HD-1500、MD シリーズ（onboard software）	全バージョン(確認中)	CVE-2026-109618 CVE-2026-109619	**影響あり**	評価中。製品固有の情報が公開されるまで、以下の推奨される緩和策を適用してください。
Automation Control Environment（ACE）	全バージョン(確認中)	CVE-2026-109618 CVE-2026-109619	**調査中**	評価を進行中です。製品固有の情報が公開されるまで、以下の推奨される緩和策を適用してください。
SmartController EX／eMotionBlox（eMB）ロボットコントローラ（i4、eCobra、Viper、Quattro）	全バージョン(確認中)	CVE-2026-109618 CVE-2026-109619	**調査中**	評価を進行中です。製品固有の情報が公開されるまで、以下の推奨緩和策を適用してください。

*本情報の発行日時点。

4. 推奨緩和策

これらの脆弱性を完全に修正するには、PHP を更新する必要があります。オムロン ロボティクスが製品固有の修正プログラムを公開するまで、顧客は悪用のリスクを低減するため、以下の対策を適用する必要があります。

1. ロボットコントローラ、モバイルロボット、フリート管理サーバー、およびエンジニアリングワークステーションがインターネットからアクセスできないことを確認してください。
2. ファイアウォールを使用してロボットおよび制御システムのネットワークを業務ネットワークから分離し、Web インターフェースおよび設定インターフェースへのアクセスを許可されたホストのみに制限してください。
3. リモートアクセスが必要な場合は、最新バージョンに更新された仮想プライベートネットワーク（VPN）などの安全な方法を使用してください。
4. Web および設定インターフェースを監視し、想定外のリクエスト、クラッシュ、またはワーカープロセスの再起動がないか確認してください。これらは悪用の試みを示している可能性があります。
5. オムロン ロボティクスのソフトウェアと PHP（例：サードパーティ製 Web アプリケーション）を併用してホストする顧客管理サーバーについては、PHP を 8.5.12、8.4.27、8.3.36、または 8.2.35 に更新するか、オペレーティングシステムのベンダーから修正済みの配布パッケージを入手してください。

5. 一般的なセキュリティに関する推奨事項

オムロン ロボティクスは、以下の業界におけるサイバーセキュリティのベストプラクティスを強く推奨します。

- 制御システムおよびロボットシステムのネットワークとリモートデバイスは、ファイアウォールの内側に配置し、業務用ネットワークから分離してください。
- 権限のない者がロボット、コントローラー、周辺機器およびネットワークにアクセスできないよう、物理的なアクセス制御を導入してください。
- プログラミングソフトウェアまたはエンジニアリングソフトウェアは、当該デバイス用に意図されたネットワーク以外には決して接続しないでください。
- 端末またはこれらのネットワークに接続されたノードで使用する前に、すべてのリムーバブルメディア（USB ドライブなど）をスキャンしてください。
- すべての制御システム機器についてネットワークへの露出を最小限に抑え、インターネットからアクセスできないようにしてください。
- IEC 62443 に準拠した多層防御のアプローチを適用し、第三者製ソフトウェアコンポーネント（SBOM）を含む最新の資産インベントリを維持してください。

6. 参考文献

- PHP セキュリティアナウンスメント：https://www.php.net/archive/2026.php#2026-10-21-5

7. 詳細情報

本書は、特定された脆弱性の概要およびその軽減に必要な対策を示すものであり、オムロンの脆弱性対応方針に従って発行されています。脆弱性の報告または追加情報のご請求については、オムロン PSIRT までご連絡ください。

- **脆弱性情報：Vulnerability Advisory & Security Updates**
- **PSIRT 連絡先：オムロン脆弱性窓口(PSIRT)**
- **地域サポート：**オムロン ロボティクスの営業担当者またはサービス担当者にお問い合わせください。

8. 法的免責事項

本情報および本書に含まれる情報は、商品性または特定目的への適合性に関する保証を含め、明示的または黙示的を問わず、いかなる種類の保証も伴わず、「現状有姿」で提供されます。OMRON は、本情報が特定された状況を解決することを保証しません。いかなる場合も、OMRON は、本情報の使用に起因するいかなる損害についても責任を負いません。お客様は、実際に存在する、または潜在的なセキュリティ脆弱性による影響を評価する責任を負います。OMRON は、いつでも本情報を更新または変更する権利を留保します。

9. 改訂履歴

バージョン	日付	説明
1.0	2026/11/2	初版リリース。調査対象製品：FLOW Core／Fleet Manager、AMR（LD、HD、MD シリーズ）、ACE、SmartController EX／eMB コントローラ。