# シスコ製品に影響を与える PHP の脆弱性：2026 年 10 月




Advisory ID : cisco-sa-php-october26-Jj384Daq
初公開日 : 2026-10-21 19:12
注: : 2026-11-06 14:21
バージョン 1.11 : Final
回避策 : Yes
Cisco Bug ID :

CVE-2026-109618
CVE-2026-109619

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

## 概要

10 月 21 日、PHP Foundation は、次の 2 つの緊急と評価された脆弱性に対処する PHP の重大なセキュリティリリースの公開を発表しました。

- CVE-2026-109618：OOM の破損による RCE
- CVE-2026-109619：古いグローバル状態による RCE

これらの脆弱性の詳細については、アドバイザリ GHSA-w8hw-w9fx-j79w および GHSA-6wmf-4rv5-p3rp を参照してください。これらの脆弱性は PHP2shell と呼ばれています。

Splunk の製品およびサービスに関する詳細については、「Vulnerabilities in PHP (CVE-2026-109618, CVE-2026-109619) on Splunk Products - October 2026」を参照してください。

重要：このアドバイザリに記載されていない製品については、シスコの調査によると、当該製品はこの脆弱性の影響を受けないことが確認されています。

このアドバイザリは、追加情報が利用可能になり次第、更新されます。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-php-october26-Jj384Daq

## 該当製品

シスコは製品ラインを調査して、この脆弱性により影響を受ける可能性がある製品を特定しました。

「脆弱性のある製品」セクションで、該当する各製品またはサービスの Cisco Bug ID を示します。これらのバグは、Cisco バグ検索ツールから確認でき、プラットフォーム固有の追加情報（回避策（利用可能な場合）および修正済みソフトウェアリリースなど）が含まれています。

### 脆弱性のある製品

次の表に、本アドバイザリに記載された脆弱性の影響を受けるシスコ製品を示します。将来のソフトウェア リリース日が示されている場合、その日付はこのアドバイザリの上部にある最終更新日時点でシスコが把握しているすべての情報に基づいた日付になります。このソフトウェア リリースの日付は、試験結果や優先される機能や修正の提供等いくつかの理由により変更される場合があります。詳細については、関連するシスコのバグを参照してください。

重要：このアドバイザリに記載されていない製品については、シスコの調査によると、当該製品はこの脆弱性の影響を受けないことが確認されています。

| シスコ製品 | Cisco Bug ID | 修正済みリリースが利用可能 |
|---|---|---|
| ワイヤレス | | |
| 超高信頼ワイヤレスバックホール（URWB）[1、2] Unified Industrial Wireless ソフトウェア | CSCwx37073 | 26.2.1.9 |
| 音声およびユニファイド コミュニケーション デバイス | | |
| Expressway シリーズ[2] | CSCwx37062 | 15.5.21 |
| Expressway Select シリーズ[2] | CSCwx37062 | 15.5.21 |
| ネットワークおよびコンテンツ セキュリティ デバイス | | |
| Duo Access Gateway | | 3.2.0 Duo Access Gateway - リリースノート |
| Identity Services Engine (ISE) Portal Builder | | 修正が展開されており、お客様のアクションは不要。 |

1. この製品の場合、脆弱性をエクスプロイトするには、攻撃者が管理者として認証されている必要があります。その結果、CVSS ベクトルは CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H となり、CVSS スコアは 6.6 になります。
2. この製品には回避策があります。詳細については、Bug ID の「 回避策」セクションを参照してください。

### 脆弱性を含んでいないことが確認された製品

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

| アプリケーション オブザーバビリティ |
| --- |
| AppDynamics Enterprise Console |
| AppDynamics On-Premises Secure Application |
| AppDynamics PHP エージェント |
| AppDynamics 仮想アプライアンス |
| ネットワークおよびコンテンツ セキュリティ デバイス |
| AI Defense（ハイブリッドオンプレミス展開用） |
| コンテンツセキュリティ管理アプライアンス(SMA) |
| E メール セキュリティ アプライアンス（ESA） |
| Hypershield |
| Identity Services Engine（ISE） |
| ISE パッシブ ID コネクタ |
| Secure Firewall 適応型セキュリティアプライアンス |
| Secure Firewall Management Center |
| Secure Firewall Threat Defense |
| ネットワーク管理とプロビジョニング |
| Business Process Automation（BPA） |
| Catalyst Center（旧 DNA Center） |
| Catalyst SD-WAN Manager |
| Common Services Platform Collector（CSPC） |
| CX エージェント |
| Evolved Programmable Network Manager（EPNM） |
| Nexus Dashboard |
| Catalyst SD-WAN Analytics |
| Catalyst SD-WAN Controller |
| Catalyst SD-WAN Portal |
| Catalyst SD-WAN Validator |
| Software Defined-Application Visibility and Control（SD-AVC） |
| Software Defined-Application Visibility and Control（SD-AVC）クラウドコネクタ |
| WAN Automation Engine（WAE） |
| Routing and Switching - Enterprise and Service Provider |
| ASR 5000 シリーズ ソフトウェア（StarOS） |

| |
|---|
| Catalyst 1300 シリーズ スイッチ |
| IOS ソフトウェア |
| IOS XE ソフトウェア |
| IOS XR ソフトウェア |
| NX-OS ソフトウェア |
| Policy Suite（CPS） |
| Ultra Packet Core - ポリシー制御機能（PCF） |
| Ultra Packet Core - Subscriber Microservices Infrastructure |
| Ultra Packet Core - ユーザープレーン機能 |
| Ultra Packet Core - Converged Policy and Charging |
| ユニファイド コンピューティング |
| すべての UCS ソフトウェア |
| ビデオ、ストリーミング、TelePresence、およびトランスコーディング デバイス |
| Meeting Management（CMM） |
| Meeting Server（CMS） |
| Cisco クラウドホステッドサービス |
| AppDynamics SaaS Secure Application |
| Duo |
| IoT Control Center |
| Multicloud Defense |
| OpenDNS |
| Secure Access |
| Secure Connect |
| Cisco Secure Email Cloud Gateway |
| Secure Email Encryption Service（CRES） |
| Secure Email Threat Defense（ETD） |
| Security Cloud Control |
| Security Cloud Control - Firewall Management（旧 Cisco Defense Orchestrator） |
| Slido |
| ThousandEyes |
| Umbrella |
| Umbrella DNS リゾルバ |
| Vulnerability Management（旧 Kenna.VM） |
| Webex アプリケーション |

| |
|---|
| Webex AI Agent |
| Webex Calling |
| Webex Collaboration Control Hub |
| Webex Contact Center |
| Webex Contact Center Enterprise |
| Webex Events |
| Webex Meetings |
| Webex Web SDK |
| Cisco のサービス |
| CX Cloud |
| IQ |
| IQ-Link |
| SD-WAN Cloud OnRamp |
| Smart Software Manager（SSM）On-Prem |
| Meraki デバイス |
| Meraki ダッシュボード |
| Meraki MG Cellular Gateway |
| Meraki MR ワイヤレスアクセスポイント |
| Meraki MS シリーズ スイッチ |
| Meraki MT シリーズ センサー |
| Meraki MV スマートカメラ |
| Meraki MX セキュリティおよび SD-WAN アプライアンス |

重要：このアドバイザリに記載されていない製品については、シスコの調査によると、当該製品はこの脆弱性の影響を受けないことが確認されています。

## 回避策

特定のシスコ製品またはサービスに対する回避策は、このアドバイザリの「脆弱性のある製品」セクションで特定されている、関連するシスコのバグに記載されています。

## 修正済みソフトウェア

修正済みソフトウェアリリースの詳細については、このアドバイザリの「脆弱性のある製品」セクションで特定されたシスコのバグを参照してください。

ソフトウェアのアップグレードを検討する場合、お客様には、シスコ製品のアドバイザリ（「

Cisco セキュリティアドバイザリ」ページから入手可能）を定期的に確認して、脆弱性に対するリスクおよび完全なアップグレード ソリューションを把握することをお勧めします。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、このアドバイザリに記載されている脆弱性に関する公式発表が行われていることを把握しています。

シスコ製品に対するこの脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

## 送信元

これらの脆弱性は PHP Foundation によって公開されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-php-october26-Jj384Daq

## 改訂履歴

| バージョン | 説明 | セクション | Status | 日付 |
|---|---|---|---|---|
| 1.11 | Ultra-Reliable Wireless Backhaul(URWB)とUnified Industrial Wireless Softwareをアップデート | 該当製品 | Final | 2026年11月6日 |
| 1.10 | ISE Portal Builder の修正ステータスと、超高信頼ワイヤレスバックホール（URWB）および Unified Industrial Wireless ソフトウェアの修正済みリリースを更新。脆弱性を含んでいないことが確認された製品に Webex Events を追加。 | 該当製品 | Final | 2026 年 10 月 30 日 |
| 1.9 | 超高信頼ワイヤレスバックホール（URWB）および Unified Industrial Wireless ソフトウェアの修正プログラムの提供日を更新。 | 該当製品 | Final | 2026 年 10 月 28 日 |
| 1.8 | 「脆弱性のある製品」と「脆弱性が存在しないことが確認された製品」を更新。 | 該当製品 | Final | 2026 年 10 月 27 日 |

| バージョン | 説明 | セクション | Status | 日付 |
|---|---|---|---|---|
| 1.7 | 調査中の製品、脆弱性を含んでいないことが確認された製品を更新。修正済みソフトウェアのリリースに関する情報を更新。 | 該当製品 | 暫定 | 2026 年 10 月 26 日 |
| 1.6 | 回避策が利用可能であることを示すために更新。調査中の製品、脆弱性を含んでいないことが確認された製品を更新。 | ヘッダー、該当製品 | 暫定 | 2026 年 10 月 23 日 |
| 1.5 | 調査中の製品、脆弱性を含んでいないことが確認された製品を更新。このアドバイザリに記載されていない製品は、この脆弱性の影響を受けないと見なされることを説明する記述を追加。 | まとめ、影響を受ける製品 | 暫定 | 2026 年 10 月 23 日 |
| 1.4 | 調査中の製品、脆弱性を含んでいないことが確認された製品を更新。 | 該当製品 | 暫定 | 2026 年 10 月 22 日 |
| 1.3 | Splunk アドバイザリのリンクを追加。「調査中の製品」、「脆弱性のある製品」、「脆弱性が存在しないことが確認された製品」を更新。 | まとめ、影響を受ける製品 | 暫定 | 2026 年 10 月 22 日 |
| 1.2 | 調査中の製品、脆弱性を含んでいないことが確認された製品を更新。 | 該当製品 | 暫定 | 2026 年 10 月 22 日 |
| 1.1 | 「脆弱性のある製品」と「脆弱性が存在しないことが確認された製品」を更新。 | 該当製品 | 暫定 | 2026 年 10 月 21 日 |
| 1.0 | 初版リリース | — | 暫定 | 2026 年 10 月 21 日 |

# 利用規約

## ソフトウェアのダウンロードおよびテクニカルサポート

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、マイデバイス（My Devices）ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。 無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

ソフトウェアのアップグレードを検討する際には、関連するシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

## 利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。本セキュリティアドバイザリの最新版については、シスコ セキュリティ アドバイザリ ページをご覧ください。Cisco Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを評価します。詳細については、シスコのセキュリティ脆弱性ポリシーを参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。