シスコ製品に影響するPHPの脆弱性：2026年11月



Advisory ID : cisco-sa-phpaftershell-nov-2026-kT9pL4Xe
初公開日 : 2026-11-23 20:20
注: : 2026-11-24 19:47
バージョン 1.1 : Interim
回避策 : No workarounds available
Cisco Bug ID :

CVE-2026-126714

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

2026年11月19日、PHP Foundationは、リモートコード実行の原因となる可能性のある重大な脆弱性に対処するセキュリティ修正プログラムの提供を発表しました。この脆弱性は、CVE-2026-126714 によって識別されています。

この脆弱性の詳細については、アドバイザリGHSA-fm2m-fjf5-v3cpを参照してください。 この脆弱性はphpAfterShellで参照されています。

Splunk製品および製品の詳細については、「Splunk製品に影響するPHPの脆弱性 – 2026年11月」を参照してください。

このアドバイザリは、追加の情報が入手可能になり次第、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-phpaftershell-nov-2026-kT9pL4Xe

該当製品

シスコでは、この脆弱性の影響を受ける製品を判断するために、製品ラインを調査中です。調査の進捗に応じて、シスコはこのアドバイザリを更新し、影響を受ける製品に関する情報を提供します。

シスコが製品がこの脆弱性の影響を受けると判断した場合、最初に修正されたリリースを次の表に示します。将来のリリース日が示されている場合、この日付はアドバイザリ上部の最終更新日の時点でシスコが把握しているすべての情報に基づいた見積もりです。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Cisco Bug IDを参照してください。

シスコの優先製品のステータス

次の表に、シスコの優先製品と、本アドバイザリに記載された脆弱性の影響に対する調査の状況を示します。追加情報が入手可能になり次第、この表は更新されます。

シスコ製品	ステータスまたはバグID	修正済みリリース情報
Catalyst Center	影響はありません	-
Catalyst SD-WAN Manager	影響はありません	-
Catalyst SD-WANバリデータ	影響はありません	-
Catalyst SD-WANコントローラ	影響はありません	-
Identity Services Engine（ISE）	影響はありません	-
IOS XE ソフトウェア	影響はありません	-
IOS XR ソフトウェア	影響はありません	-
Nexus Dashboard	影響はありません	-
NX-OS ソフトウェア	影響はありません	-
Cisco Secure Firewall 適応型セキュリティアプライアンス（ASA）ソフトウェア	影響はありません	-
Cisco Secure Firewall Management Center（FMC）ソフトウェア	影響はありません	-
Cisco Secure Firewall Threat Defense（FTD）ソフトウェア	影響はありません	-
UCS Central Software	影響はありません	-
UCS Director	影響はありません	-

該当するシスコ製品のステータス

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。追加情報が入手可能になり次第、この表は更新されます。

重要：この表には、該当するソフトウェアコンポーネントが含まれていることが確認されているシスコ製品のみが記載されています。

シスコ製品	ステータスまたはバグID	修正済みリリース情報
ワイヤレス		

シスコ製品	ステータスまたはバグ ID	修正済みリリース情報
信頼性の高いワイヤレスバックホール(URWB) Unified Industrial Wirelessソフトウェア	CSCwx94501	26.2.1b（2026年12月） 27.1.1（2027年3月）
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	CSCwx94499	X15.6（未定）
Expressway Selectシリーズ	CSCwx94499	X15.6（未定）
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アクセスゲートウェイ		3.3.0 Duo Access Gateway – リリースノート

脆弱性を含んでいないことが確認された製品

このアドバイザリの該当製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

回避策

特定のシスコ製品に対する回避策は、適切なCisco Bugとして文書化され、それぞれこのアドバイザリの「該当製品」セクションで特定されます。

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「該当製品」セクションに記載されているCisco Bug ID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際は、Cisco Security Advisoriesページで入手でき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完全なアップグレードソリューション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。

シスコの 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検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

送信元

この脆弱性は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-phpaftershell-nov-2026-kT9pL4Xe

改訂履歴

バージョン	説明	セクション	Status	日付
1.1	Cisco Duo Access GatewayおよびCisco Expresswayの修正済みリリース情報を更新。	該当製品	暫定	2026年11月24日
1.0	初版リリース	—	暫定	2026年11月23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。