Cisco Expresswayシリーズセキュリティ強化リリース：2026年10月

High

Advisory ID : cisco-sa-exwy-hardening-FhcqBVcs
初公開日 : 2026-10-21 16:00
注: : 2026-10-27 14:45
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco Bug ID :

CVE-2026-76497
CVE-2026-76496
CVE-2026-76495
CVE-2026-76494
CVE-2026-76493
CVE-2026-76492
CVE-2026-76491
CVE-2026-76490

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

予防的なセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、Cisco Expresswayシリーズソフトウェアエンジニアリングチームは、包括的な社内セキュリティレビューを実施しました。このレビュー結果、社内で発見された複数の脆弱性に対処するソフトウェアのセキュリティ強化リリースが公開されました。

これらの脆弱性は内部テストで発見されたものであり、現時点でエクスプロイトの事例は確認されていません。パッチの適用と開示プロセスの合理化を支援するために、シスコでは、これらの問題を基盤となる脆弱性クラス(Common Weakness Enumeration(CWE))別にグループ化し、各CWEグループにCommon Vulnerabilities and Exposures ID(CVE ID)を1つ割り当てています。

Cisco Expresswayシリーズは、Cisco Expressway Core(Expressway-C)デバイスとCisco Expressway Edge(Expressway-E)デバイスを指します。

注：シスコは、本リリースで対処される個々の脆弱性に関する追加詳細情報を提供するセキュリティアドバイザリを個別に公開することができます。

シスコはこれらの脆弱性に対処するソフトウェアアップデートをリリースしました。これらの脆弱性に対処する回避策はありません。

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-exwy-hardening-FhcqBVcs

本アドバイザリは一連のアドバイザリの一部です。アドバイザリの完全なリストおよび各アドバイザリへのリンクについては、「Cisco Advance Notification for Publication of October 21, 2026, Security Advisories」を参照してください。

該当製品

脆弱性のある製品

これらの脆弱性は、デバイス設定に関係なく、仮想バージョンとアプライアンスバージョンの両方でCisco Expressway-CとCisco Expressway-Eに影響を与えます。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの修正済みソフトウェア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

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

詳細

次の表に、このソフトウェア強化リリースで対処される脆弱性クラスの概要を示します。各 CVE ID に割り当てられる CVSS スコアは、その特定の CWE カテゴリ内で最も影響の大きい 1 つの根本的な脆弱性がもたらす可能性がある最大のシビラティ（重大度）を表しています。

CVE ID	CVSS最高スコア	脆弱性クラス（最高レベルのCWE）	説明
CVE-2026-76490	8.6	CWE-787	範囲外の書き込み
CVE-2026-76491	8.6	CWE-617	到達可能な主張
CVE-2026-76492	8.6	CWE-476	ヌルポインタの逆参照
CVE-2026-76493	8.6	CWE-248	キャッチされない例外
CVE-2026-76494	7.8	CWE-94	コード生成の制御が不適切（コードインジェクション）
CVE-2026-76495	7.8	CWE-732	重要なリソースの権限の割り当てが正しくない

CVE ID	CVSS最高スコア	脆弱性クラス（最高レベルのCWE）	説明
CVE-2026-76496	7.8	CWE-59	ファイルアクセスの前の不適切なリンク解決（リンクに続く）
CVE-2026-76497	7.8	CWE-377	安全でない一時ファイル

回避策

これらの脆弱性に対処する回避策はありません。

修正済みソフトウェア

これらの脆弱性を修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正リリース

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこれらの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco Expressway シリーズのリリース	第 1 修正済みリリース
X14以前	修正済みリリースに移行。
X15.5.3 以前	X15.5.20

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とその公表は確認しておりません。

送信元

これらの脆弱性は、既存のテストプロセスおよびフロンティアの AI モデルを使用した内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-exwy-hardening-FhcqBVcs

改訂履歴

バージョン	説明	セクション	Status	日付
1.1	CWE-787の説明を更新。	詳細	Final	2026年10月27日
1.0	初版リリース	—	Final	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。