Cisco Expressway シリーズのクロスサイト リクエスト フォージェリの脆弱性

アドバイザリーID : cisco-sa-expressway-csrf-KnnZDMj3
初公開日 : 2024-02-07 16:00
最終更新日 : 2024-02-12 17:55
バージョン 1.1 : Final
CVSSスコア : 9.6
回避策 : No workarounds available
Cisco バグ ID : CSCwa25074 CSCwa25099 CSCwa25100

CVE-2024-20254
CVE-2024-20255
CVE-2024-20252

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco Expresswayシリーズの複数の脆弱性により、認証されていないリモートの攻撃者がクロスサイトリクエストフォージェリ(CSRF)攻撃を実行する可能性があります。これにより、攻撃者が該当デバイスで任意のアクションを実行する可能性があります。

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

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

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ています。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-expressway-csrf-KnnZDMj3

該当製品

脆弱性のある製品

CVE-2024-20254 および CVE-2024-20255：これらの脆弱性は、デフォルト設定の Cisco Expressway シリーズ デバイスに影響します。

CVE-2024-20252：この脆弱性は、クラスタデータベース（CDB）API 機能が有効になっている場合、Cisco Expressway シリーズ デバイスに影響します。この機能は、Cisco Expresswayシリーズリリース14.2以降ではデフォルトで無効になっています。Cisco Expresswayシリーズリリース14.2よりも前のリリースでは、クラスタデータベース(CDB)API機能はデフォルトで有効になっており、無効にすることはできません。

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

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2024-20252 および CVE-2024-20254：Cisco Expressway シリーズのクロスサイト リクエスト フォージェリの脆弱性

Cisco Expressway シリーズ デバイスの API にある 2 つの脆弱性により、認証されていないリモート攻撃者が、該当システムで CSRF 攻撃を実行できる可能性があります。

これらの脆弱性は、該当システムの Web ベース管理インターフェイスの CSRF 保護が不十分なことに起因します。攻撃者は、API のユーザーを、細工されたリンクにアクセスするように誘導することで、これらの脆弱性をエクスプロイトする可能性があります。不正利用に成功すると、攻撃者は該当ユーザの特権レベルで任意のアクションを実行できる場合があります。影響を受けるユーザーが管理者権限を持っている場合、これらのアクションには、システム設定の変更と新しい特権アカウントの作成が含まれる可能性があります。

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ています。これらの脆弱性に対処する回避策はありません。

バグ ID：CSCwa25099 および CSCwa25100
CVE ID：CVE-2024-20252 および CVE-2024-20254
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9.6
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVE-2024-20255：Cisco Expressway シリーズのクロスサイト リクエスト フォージェリの脆弱性

Cisco Expressway シリーズの API にある脆弱性により、認証されていないリモート攻撃者が、該当システムで CSRF 攻撃を実行できる可能性があります。

この脆弱性は、該当システムの Web ベース管理インターフェイスの CSRF 保護が不十分なことに起因します。攻撃者は、API のユーザーを、巧妙に細工されたリンクにアクセスするように誘導することで、この脆弱性をエクスプロイトする可能性があります。不正利用に成功すると、攻撃者は該当ユーザの特権レベルで任意のアクションを実行できる場合があります。影響を受けるユーザーが管理者権限を持っている場合、これらのアクションにはシステム設定の上書きが含まれる可能性があります。これにより、システムがコールを適切に処理できなくなり、サービス妨害（DoS）状態が発生する可能性があります。

シスコはこ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ています。この脆弱性に対処する回避策はありません。

バグ ID：CSCwa25074
CVE ID：CVE-2024-20255
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.2
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:L

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェ

ア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ 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。

サービス契約をご利用でないお客様

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 TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）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。

修正済みリリース

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	First Fixed Release（修正された最初のリリース）
14 より前	修正済みリリースに移行。
14	14.3.41
15	15.0.01

1. 完全な修正を有効にするには、 Cisco Expressway の管理者ガイドで説明されているように、xconfiguration Security CSRFProtection status : "Enabled" コマンドを実行します。

Cisco TelePresence Video Communication Server

Cisco TelePresence Video Communication Server（VCS）は、サポート終了日を迎えており、

Cisco Expressway シリーズのアドバイザリには含まれなくなりました。シスコは、このアドバイザリで説明している脆弱性に対処するための Cisco TelePresence VCS のソフトウェアアップデートをリリースしておらず、リリースする予定もありません。お客様には、Cisco TelePresence VCS のサポート終了通知を参照することをお勧めします。

https://www.cisco.com/c/en/us/products/collateral/unified-communications/telepresence-video-communication-server-vcs/eos-eol-notice-c51-743969.html

ソフトウェアの移行を検討する際は、[シスコ セキュリティ アドバイザリ（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の有無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。

いずれの場合でも、新しいソフトウェアがお客様のネットワークニーズに十分対応していること、新しいデバイスに十分なメモリが搭載されていること、および現在のハードウェアとソフトウェアの構成が新しい製品で引き続き適切にサポートされることを確認してください。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。

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された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。

出典

CVE-2024-20252 および CVE-2024-20254：これらの脆弱性は、Cisco Advanced Security Initiatives Group（ASIG）の Jason Crowder による内部セキュリティテストで発見されました。

CVE-2024-20255：この脆弱性は、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-expressway-csrf-KnnZDMj3

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	脆弱性が存在する製品情報と修	「脆弱性のある製品」および	Final	2024年2月

バージョン	説明	セクション	ステータス	日付
	正済みリリースを明確化。	「修正済みリリース」		12日
1.0	初回公開リリース	—	Final	2024 年 2 月 7 日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、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。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。