Cisco Expressway シリーズおよび Cisco TelePresence Video Communication Server の脆弱性

Medium

アドバイザリーID : cisco-sa-expressway-filewrite-bsFVwueV
初公開日 : 2022-05-18 16:00
最終更新日 : 2023-01-17 20:24
バージョン 1.2 : Final
CVSSスコア : 5.5
回避策 : No workarounds available
Cisco バグ ID : CSCvz71486 CSCwa25061 CSCwa25106

CVE-2022-20807
CVE-2022-20806
CVE-2022-20809

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シリーズおよびCisco TelePresence Video Communication Server(VCS)のAPIおよびWebベースの管理インターフェイスにおける複数の脆弱性により、認証されたリモートの攻撃者が該当デバイスにファイルを書き込んだり、機密情報を開示したりする可能性があります。

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-filewrite-bsFVwueV

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性はCisco ExpresswayシリーズおよびCisco TelePresence VCSに影響を与えていました。

注：CVE-2022-20806およびCVE-2022-20807では、デフォルト設定に脆弱性が存在します。CVE-2022-20809の影響を受けるのは、デバッグロギングが有効になっているシスコ製品だけです。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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-2022-20806:Cisco ExpresswayシリーズおよびCisco TelePresence VCSにおける任意のファイル書き込みの脆弱性

Cisco ExpresswayシリーズおよびCisco TelePresence Video Communication Server(VCS)のクラスタデータベースAPIにおける脆弱性により、アプリケーションに対する読み取り/書き込み権限を持つ認証されたリモート攻撃者が、機密情報を取得し、該当デバイスに部分的なサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、ユーザーが指定したコマンド引数の入力検証が不十分であることに起因します。攻撃者は、読み取り/書き込み権限を使用してデバイスに認証され、巧妙に細工されたコマンドを発行することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は基盤となるオペレーティングシステム上の任意のファイルを、システムのパフォーマンスに影響を与える速度で読み取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:CSCvz71486
CVE ID：CVE-2022-20806
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.5
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:L

CVE-2022-20807:Cisco ExpresswayシリーズおよびCisco TelePresence VCS XMLの外部エンティティインジェクションの脆弱性

Cisco ExpresswayシリーズおよびCisco TelePresence Video Communication Server(VCS)のファイル解析ロジックにおける脆弱性により、読み取り/書き込み権限を持つ認証されたリモートの攻撃者が、該当デバイスの機密情報を取得できる可能性があります。

この脆弱性は、特定のXMLファイルを解析する際のXML外部エンティティ(XXE)エントリの不適切な処理に起因します。攻撃者は、外部エンティティへの参照を含む巧妙に細工されたXMLファイルをアップロードすることで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はローカルシステムからファイルを取得し、影響を受けるシステムで機密情報を開示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:CSCwa25061
CVE ID：CVE-2022-20807
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.9
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVE-2022-20809:Cisco ExpresswayシリーズおよびCisco TelePresence VCSにおける任意のファイル書き込みの脆弱性

Cisco ExpresswayシリーズおよびCisco TelePresence Video Communication Server(VCS)のロギングコンポーネントの脆弱性により、認証されたリモートの攻撃者が該当システムの機密情報をクリアテキストで表示できる可能性があります。

この脆弱性は、特定のログに暗号化されていないクレデンシャルが保存されることに起因します。攻撃者は、該当システムのログにアクセスすることで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は共有デバイスの他のユーザのクレデンシャルを表示できる可能性があります。この脆弱性は、デバイスでデバッグロギングが有効になっている場合にのみ発生します。

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:CSCwa25106
CVE ID：CVE-2022-20809
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.3
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

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

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。

修正済みリリース

発行時点では、次の表に記載されているリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列にはシスコソフトウェアリリースが、右の列に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リリースが示されています。

Cisco Expressway シリーズおよび Cisco TelePresence VCS リリース	First Fixed Release（修正された最初のリリース）
14.0 より前	修正済みリリースに移行。
14.0	14.0.7

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やその公表は確認しておりません。

出典

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。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-filewrite-bsFVwueV

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	メモのCVE IDを更新。	脆弱性が存在する製品	Final	2023年1月17日
1.1	CVE-2022-20809の影響を受けるのは、デバッグロギングが有効になっているシスコ製品のみであることを示すように更新されました。	脆弱性が存在する製品	Final	2022年5月24日
1.0	初回公開リリース	—	Final	2022年5月18日

利用規約

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。