Cisco FinesseのWebベース管理インターフェイスの脆弱性

Medium

アドバイザリーID : cisco-sa-finesse-ssrf-rfi-Um7wT8Ew
初公開日 : 2024-06-05 16:00
最終更新日 : 2024-06-06 17:54
バージョン 1.1 : Final
CVSSスコア : 7.2
回避策 : No workarounds available
Cisco バグ ID : CSCwh95276 CSCwh95292

CVE-2024-20405
CVE-2024-20404

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 FinesseのWebベース管理インターフェイスにおける複数の脆弱性により、認証されていないリモートの攻撃者が、Remote File Inclusion(RFI)の脆弱性を不正利用したStored Cross Site Scripting(XSS)攻撃や、該当システムに対するServer-Side Request Forgery(SSRF)攻撃を実行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-finesse-ssrf-rfi-Um7wT8Ew

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性はデフォルト設定のCisco Finesseに影響を与えていました。

Cisco Finesseにバンドルされている可能性がある次のシスコ製品も、これらの脆弱性の影響を受けます。

- Packaged Contact Center Enterprise（Packaged CCE）
- Unified Contact Center Enterprise（Unified CCE）
- Unified Contact Center Express（Unified CCX）
- Unified Intelligence Center

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、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受ける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-2024-20404:Cisco Finesse SSRFの脆弱性

Cisco FinesseのWebベース管理インターフェイスの脆弱性により、認証されていないリモートの攻撃者が該当システムにSSRF攻撃を実行する可能性があります。

この脆弱性は、該当システムに送信される特定のHTTP要求に対するユーザ入力の検証が不十分であることに起因します。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、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、攻撃者は該当デバイスに関連付けられているサービスの限られた機密情報を取得でき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。

注：セキュリティ影響評価(SIR)は、攻撃者がアクセスできる情報の範囲が限られているため、中レベルです。

バグID:CSCwh95292
CVE ID：CVE-2024-20404
重大度インパクト評価(SIR)：中
CVSS ベーススコア：7.2
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N

CVE-2024-20405:Cisco FinesseがRFIの脆弱性によりXSSを格納

Cisco FinesseのWebベース管理インターフェイスの脆弱性により、認証されていないリモートの攻撃者がRFIの脆弱性を不正利用してストアドXSS攻撃を実行する可能性があります。

この脆弱性は、該当デバイスに送信される特定のHTTP要求に対するユーザ入力の検証が不十分であることに起因します。攻撃者は、巧妙に細工されたリンクをクリックするようにユーザを誘導することにより、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、攻撃者は影響を受けるインターフェイスに関連する任意のスクリプトコードを実行したり、影響を受けるデバイスの機密情報にアクセスしたり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:CSCwh95276
CVE ID：CVE-2024-20405
重大度インパクト評価(SIR)：中
CVSS ベーススコア：4.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/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、次の表に示す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Ciscoソフトウェアリリースが、右の列にはそのリリースが本アドバイザリに記載された脆弱性の影響を受けるかどうか、またどのリリースにこれらの脆弱性に対する修正が含まれているかを示します。

Cisco Finesseリリース	First Fixed Release（修正された最初のリリース）
11.6(1) ES11以前	修正済みリリースに移行。
12.6(2) ES01以前	12.6(2) ES03

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

シスコは、これらの脆弱性を報告していただいたAbd El Rahman Ezzat氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew

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	ソース名を更新。	出典	Final	2024年6月6日
1.0	初回公開リリース	—	Final	2024年6月5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。