

Cisco Finesseサーバ側の要求フォージェリの脆弱性



Advisory ID : cisco-sa-finesse-ssrf-mmSuyugS

[CVE-2026-20362](#)

初公開日 : 2026-10-07 16:00

バージョン 1.0 : Final

CVSSスコア : [7.2](#)

回避策 : No workarounds available

Cisco Bug ID : [CSCwv36526](#)

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

Cisco FinesseのWebベースの管理インターフェイス(Web GUI)における脆弱性により、認証されていないリモートの攻撃者が、該当デバイスを経由してサーバ側の要求フォージェリ(SSRF)攻撃を実行する可能性があります。

この脆弱性は、特定の HTTP 要求の不適切な入力検証に起因します。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。

シスコでは、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する予定です。こ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-mmSuyugS>

該当製品

脆弱性がある製品

この脆弱性は、デバイスの設定に関係なく、Cisco Finesseに影響を与えます。

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)

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[脆弱性が存在する製品](#)セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性がCisco Unified Intelligence Centerには影響を与えないことを確認しました。

回避策

こ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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を修正し、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示します。右側の列は、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。このセクションで示すように、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 Finesseリリース	第 1 修正済みリリース
12.6 以前	修正済みリリースに移行。
15.0	15.0(1) SU3 (2027年2月)

Cisco Packaged CCEおよびUnified CCEリリース	第 1 修正済みリリース
15.0 よりも前	修正済みリリースに移行。
15.0	15.0(1)ES202701 (2027年1月)

Cisco Unified CCX リリース	第 1 修正済みリリース
12.5 以前	修正済みリリースに移行。
15.0	15.0(1) SU2 (2027年2月)

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は、このアドバイザリに記載されている脆弱性の公式発表があることを認識しています。

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は確認しておりません。

出典

シスコは、この脆弱性を報告していただいたHorizon3社のNoah King氏とBrandon Peterson氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-mmSuyugS>

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2026年10月7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。