Cisco Unified Communications Managerサーバ側の要求フォージェリの脆弱性

アドバイザリーID : cisco-sa-cucm-ssrf-cXPnHcW
初公開日 : 2026-06-03 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCws67331

CVE-2026-20230

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 Unified Communications Manager(Unified CM)およびCisco Unified Communications Manager Session Management Edition(Unified CM SME)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、攻撃者は基盤となるオペレーティングシステムにファイルを書き込み、後でルートに昇格するために使用できるようになります。

注：スコアに示されているように、シスコはこのセキュリティアドバイザリのセキュリティ影響評価（SIR）に High（高）ではなく Critical（重大）を割り当てています。この脆弱性のエクスプロイトにより、攻撃者が権限をルートに昇格できる可能性があるためです。

注：この脆弱性を不正利用するには、WebDialerサービスが有効になっている必要があります。WebDialerはデフォルトで無効になっています。

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。

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-cucm-ssrf-cXPnHcW

該当製品

脆弱性のある製品

この脆弱性は、WebDialerサービスを有効にしているCisco Unified CMおよびUnified CM SME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。

WebDialerが有効になっているかどうかの確認

WebDialerが有効になっているかどうかを確認するには、次の手順を実行します。

1. Cisco Unified CM Administrationインターフェイスにログインします。
2. Navigationメニューから、Cisco Unified Serviceabilityを選択し、Goをクリックします。
3. Toolsメニューから、Control Center - Feature Servicesの順に選択します。
4. ページのCTI Servicesセクションで、Cisco WebDialer Web Serviceの現在のステータスがStartedであるか、Not Runningであるかを確認します。

ステータスがStartedの場合、WebDialerは有効です。

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。

回避策

この脆弱性に対処する回避策はありません。ただし、緩和策として、パッチを適用できるまで、管理者はWebDialerサービスを無効にすることができます。

WebDialerを無効にするには、次の手順を実行します。

1. Cisco Unified CM Administrationインターフェイスにログインします。
2. Navigationメニューから、Cisco Unified Serviceabilityを選択し、Goをクリックします。
3. Toolsメニューから、Service Activationを選択します。
4. ページのCTI Servicesセクションで、Cisco WebDialer Web Serviceチェックボックスのチェックマークを外して、Saveをクリックします。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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。この脆弱性を完全に修正し、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 Unified CM および Unified CM SME のリリース	First Fixed Release（修正された最初のリリース）
14	14SU6
15	15SU5（2026年9月）またはCOP[1]

1. パッチはバージョン固有です。詳細については、パッチに添付されている README を参照してください。

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、このアドバイザリで説明されている脆弱性に対してコンセプト実証エクスプロイトコードが利用可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

シスコは、この脆弱性を報告していただいたSSD Secure Disclosureの調査に携わった独立したセキュリティ研究者に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2026年6月3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。