Cisco Unity Connectionのリモートコード実行およびサーバ側要求偽造の脆弱性

High

アドバイザリーID : cisco-sa-unity-rce-ssrf-hENhuASy
初公開日 : 2026-05-06 16:00
バージョン 1.0 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCwq36834 CSCwq36774

CVE-2026-20035
CVE-2026-20034

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 Unity Connectionの複数の脆弱性により、リモート攻撃者が該当デバイスで任意のコードを実行したり、サーバ側の要求フォージェリ(SSRF)攻撃を実行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-unity-rce-ssrf-hENhuASy

該当製品

脆弱性のある製品

CVE-2026-20034：この脆弱性は、デバイス設定に関係なく、Cisco Unity Connectionに影響します。

CVE-2026-20035：この脆弱性は、Web Inboxが有効な場合にCisco Unity Connectionに影響します。 Web Inboxはデフォルトで有効になっています。

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。

Web Inboxが有効になっているかどうかの確認

Web Inboxが有効になっているかどうかを確認するには、次の手順に従います。

1. Cisco Unity Connection Administrationインターフェイスに接続し、Class of Serviceを選択します。
2. 事前定義されたサービスクラスとして、ボイスメールユーザCOSを選択するか、カスタムサービスクラスを選択します。
3. ライセンス取得済み機能セクションで、ユーザにWeb InboxおよびRSSフィードの使用を許可するようスクロールダウンします。

Allow Users to Use the Web Inbox and RSS Feedsボックスにチェックマークが入っている場合、この機能は有効です。

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-2026-20034:Cisco Unity Connectionのリモートコード実行の脆弱性

Cisco Unity ConnectionのWebベースの管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が該当デバイスで任意のコードを実行する可能性があります。

この脆弱性は、ユーザ指定の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 API 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rootとして任意のコードを実行し、ターゲットデバイスが完全に侵害される可能性があります。 この脆弱性を不正利用するには、攻撃者は該当デバイスで有効なユーザクレデンシャルを持っている必要があります。

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: CSCwq36774
CVE ID：CVE-2026-20034
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.8

CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2026-20035:Cisco Unity Connection SSRFの脆弱性

Cisco Unity Connection Web InboxのWeb UI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介して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要求に対する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を送信元とする任意のネットワーク要求を送信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。

バグID: CSCwq36834
CVE ID：CVE-2026-20035
セキュリティ影響評価（SIR）：高
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

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。これら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 Unity Connection リリース	First Fixed Release（修正された最初のリリース）
12.5 以前	修正済みリリースに移行。
14.0	14SU5
15.0	15SU4 またはパッチファイルの適用：[1]

Cisco Unity Connection リリース	First Fixed Release（修正された最初のリリース）
	ciscocm.cuc.V15_CSCwq36774-CSCwq36834_C0277-1.zip

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 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NATOサイバーセキュリティセンター(NCSC)のセキュリティ研究者Jahmel Harris氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-unity-rce-ssrf-hENhuASy

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5月6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。