Cisco Unity Connection ディレクトリ トラバーサルの脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20140407-CVE-2014-2145 **初公開日 :** 2014-04-07 16:02 **バージョン 1.0 :** Final **CVSSスコア :** 4.0 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCun91071	CVE-2014-2145

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 のメッセージング API の脆弱性はディレクトリ トラバーサルを実行し、許可された MIME 型を一致する任意ファイルをダウンロードする認証される、リモート攻撃者を可能にする可能性があります。

脆弱性は不十分な入力フィルタリングがあり、 *.wav* 以外のファイルタイプが許可されるので発生します。 攻撃者は Wave ファイル ダウンロードの要求によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者が許可された MIME 型を一致するシステムのファイルへのアクセスを得ることを可能にする可能性があります。

Cisco はセキュリティ通知およびリリースされたソフトウェア アップデートの脆弱性を確認しました。

この脆弱性を不正利用するために、攻撃者は目標とされたデバイスに認証する必要があります。このアクセス要件は正常なエクスプロイトの確率を減少させます。

Cisco は CVSS スコアを通してその機能エクスプロイト コード存在を示します; ただし、コードは共用利用可能であると知られていません。

該当製品

顧客は影響を受けた製品バージョンの完全なリストのための Cisco バグ ID CSCun91071 を参照するように勧告されます。

脆弱性のある製品

このアラートが最初に送達された時、Cisco Unity Connection 9.1(2) および前は脆弱でした。Cisco Unity Connection の以降のリリースはまた脆弱かもしれません。

脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

回避策

管理者は適切な更新を加えるように助言されます。

管理者は信頼されたユーザだけネットワーク アクセスをアクセスできることを許可するために助言されます。

管理者は影響を受けたシステムを監視するように助言されます。

修正済みソフトウェア

アクティブな契約を持つ Cisco カスタマはこの脆弱性のための修正を含むソフトウェア バージョンへのアップグレードの支援に関しては Cisco サポート チームに連絡する必要があります。 契約のない Cisco カスタマは支援のための *tac@cisco.com* に 1-800-553-2447 か 1-408-526-7209 でまたはメールで Cisco Technical Assistance Center に連絡することができます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20140407-CVE-2014-2145

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2014-Apr-07

利用規約

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、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。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。