Cisco Unity Connectionのクロスサイトスクリプティング、オープンリダイレクト、およびSQLインジェクションの脆弱性

Medium

アドバイザリーID : cisco-sa-unity-vulns-n2EJSbbw
初公開日 : 2026-04-15 16:00
バージョン 1.0 : Final
CVSSスコア : 6.1
回避策 : No workarounds available
Cisco バグ ID : CSCwq36822 CSCwq36828 CSCwq36796

CVE-2026-20060
CVE-2026-20061
CVE-2026-20059

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、リモート攻撃者がクロスサイトスクリプティング(XSS)攻撃、オープンリダイレクト攻撃、およびSQLインジェクション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-unity-vulns-n2EJSbbw

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性はデバイス設定に関係なく、Cisco Unity Connectionに影響を与えていました。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェア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-2026-20059:Cisco Unity ConnectionのXXS反映の脆弱性

Cisco Unity ConnectionのWebベースの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、インターフェイスのユーザに対してリフレクトXSS攻撃を実行する可能性があります。

この脆弱性は、Webベースの管理インターフェイスがユーザ入力を適切に検証しないことに起因しています。攻撃者は、ユーザーを、巧妙に細工されたリンクをクリックするように誘導することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセス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:CSCwq36822
CVE ID：CVE-2026-20059
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE-2026-20060:Cisco Unity Connectionオープンリダイレクトの脆弱性

Cisco Unity Connection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悪意のあるWebページにユーザをリダイレクトする可能性があります。

この脆弱性は、HTTP要求パラメータの不適切な入力検証に起因します。攻撃者は、ユーザーを、巧妙に細工されたリンクをクリックするように誘導することで、この脆弱性をエクスプロイト

する可能性があります。エクスプロイトに成功すると、攻撃者はユーザを悪意のあるWebページにリダイレクト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:CSCwq36828
CVE ID：CVE-2026-20060
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.7
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N

CVE-2026-20061:Cisco Unity Connection SQLインジェクションの脆弱性

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に対してSQLインジェクション攻撃を実行す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。

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HTTP(S)要求を該当デバイスのWebベース管理インターフェイスに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のデータを表示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:CSCwq36796
CVE ID：CVE-2026-20061
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/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

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。

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。中央および右の列は、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。

Cisco Unity Connection リリース	CVE-2026-20059およびCVE-2026-20061の最初の修正済みリリース	CVE-2026-20060 の最初の修正済みリリース
12.5	修正済みリリースに移行。	修正済みリリースに移行。
14	14SU6	14SU5
15	15SU4	15SU4

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や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Jahmel Harris氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-unity-vulns-n2EJSbbw

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4月15日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものでは

ありません。 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。

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。