Cisco BroadWorksアウトオブバンドブラインドXML外部エンティティインジェクションの脆弱性

High

アドバイザリーID : cisco-sa-bworks-xxe-uwUd7CEt
初公開日 : 2026-08-19 16:00
バージョン 1.0 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCwv48590

CVE-2026-20320

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 BroadWorksのOpen Client Interface(OCI)XMLパーサーの脆弱性により、認証されていないリモートの攻撃者が該当システムの機密の設定情報を読み取る可能性があります。

この脆弱性は、デフォルトで許可されている外部エンティティの解決が原因でXMLエントリが適切に解析されないことに起因しています。攻撃者は、巧妙に細工されたXMLメッセージをOpen Client Interface - Provisioning(OCI-P)サービ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Cisco BroadWorksユーザの権限を使用してファイルシステムから機密ファイル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。

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-bworks-xxe-uwUd7CEt

該当製品

脆弱性のある製品

この脆弱性は、デバイス設定に関係なく、Cisco BroadWorksの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えます。

- BroadWorks Application Delivery Platform
- BroadWorks Application Server
- BroadWorks Profile Server
- BroadWorks Xtended Services Platform

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。

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の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。

BroadWorks Application Delivery Platformリリース	First Fixed Release（修正された最初のリリース）
RI.2026.07[1]よりも前	RI.2026.07

1. Open Client Server(OCS)およびOCIOverSoap。

BroadWorks Application Serverリリース	First Fixed Release（修正された最初のリリース）
RI.2026.07より前	RI.2026.07

BroadWorks Profile Serverリリース	First Fixed Release（修正された最初のリリース）
RI.2026.07より前	RI.2026.07

BroadWorks Xtended Services Platformリリース	First Fixed Release（修正された最初のリリース）
RI.2026.07より前	RI.2026.07

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

この脆弱性を報告していただいたSandesh M Gawai氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bworks-xxe-uwUd7CEt

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8月19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。