Cisco BroadWorksアプリケーションサーバの情報漏えいの脆弱性

アドバイザリーID : cisco-sa-broad-as-inf-disc-ZUXGFFXQ
CVE-2021-1562
初公開日 : 2021-07-07 16:00
最終更新日 : 2021-07-09 18:17
バージョン 1.1 : Final
CVSSスコア : 4.3
回避策 : No workarounds available
Cisco バグ ID : CSCvv41798

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 Application ServerのXSI-Actions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システムの機密情報にアクセスできる可能性があります。

この脆弱性は、XSI-Actionsインターフェイス内でユーザが実行できる特定のコマンドの入力の検証と認可が不適切であることに起因します。攻撃者は、該当デバイスに認証され、特定のコマンドセットを発行することにより、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、攻撃者はコールセンターインスタンスに参加し、コールセンターキューからアクセスする権限のないコールを受け取る可能性があります。

このドキュメントの発行時点で、シスコはこの脆弱性に対処するCisco BroadWorks Application Serverのアップデートをリリースしていません。ただし、ファームウェアパッチは利用可能です。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-broad-as-inf-disc-ZUXGFFXQ

該当製品

脆弱性のある製品

公開時点では、この脆弱性はCisco BroadWorks Application Serverに影響を与えました。

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。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、この脆弱性の影響を受けることが分かっています。

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

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

修正済みリリース

このドキュメントの発行時点で、シスコはこの脆弱性に対処するCisco BroadWorks Application Serverのアップデートをリリースしていません。ただし、ファームウェアパッチは入手可能でした。

発行時点では、次の表に記載されている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。

左の列には、このアドバイザリに記載された脆弱性の影響を受けるシスコソフトウェアリリースが一覧表示されています。中央の列には、この脆弱性に対するパッチがリリースされたかどうか、およびパッチを検索できるリリース番号が表示されます。右側の列には、使用可能なパッチのファイル名が表示されます。

Cisco BroadWorks Application Serverリリース	release number	パッチファイル名
17.0	計画なし	—
18.0	計画なし	—
19.0	計画なし	—
20.0	計画なし	—

Cisco BroadWorks Application Serverリリース	release number	パッチファイル名
21.0	計画なし	—
22.0	22.0.2020.08	AP.as.22.0.1123.ap375453.Linux-x86_64.zip
23.0	23.0.2020.08	AP.as.23.0.1075.ap375453.Linux-x86_64.zip
24.0	24.0.2020.08	AP.as.24.0.944.ap375453.Linux-x86_64.zip

Cisco.comのSoftware Centerからファームウェアパッチをダウンロードするには、次の手順を実行します。

1. [すべてを参照（Browse All）] をクリックします。
2. Unified Communications > Cloud Calling > BroadWorks > BroadWorks Application Server [release]の順に選択します。
3. Application Patchesを選択してから、上記の表のRelease Number列にリストされている適切なリリースを選択します。
4. 上記の表の「パッチファイル名」列にリストされている適切なファイルを選択します。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broad-as-inf-disc-ZUXGFFXQ

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	パッチファイル情報を追加。	修正済みソフトウェア	Final	2021年7月9日
1.0	初回公開リリース	—	Final	2021 年 7 月 7 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。