Cisco BroadWorks SIPのDoS脆弱性

High

アドバイザリーID : cisco-sa-bw-sip-dos-mSySbrmt
初公開日 : 2025-01-22 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 : CSCwm97019

CVE-2025-20165

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SIP処理サブシステムの脆弱性により、認証されていないリモートの攻撃者が着信SIP要求の処理を停止し、その結果サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、特定のSIP要求に対する不適切なメモリ処理に起因します。攻撃者は、該当システムに大量のSIP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、SIPトラフィックを処理するCisco BroadWorks Network Serverに割り当てられたメモリを使い果たすことができます。使用可能なメモリがない場合、ネットワークサーバは着信要求を処理できなくなり、その結果、DoS状態が発生して、回復するには手動による介入が必要になります。

この脆弱性の詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

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-bw-sip-dos-mSySbrmt

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、Cisco BroadWorksに影響を与えます。

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。

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。

詳細

攻撃者がこの脆弱性を悪用するには、Cisco BroadWorks Network Serverに割り当てられたメモリを完全に飽和状態にする必要があります。管理者はこれらのサーバに任意の量のメモリを割り当てることができるため、DoS状態を発生させるために必要なSIP要求の時間と量は異なります。

管理者は使用中のメモリの現在のステータスを監視し、使用量が最大値に近づいた場合は、DoS状態を回避するためにネットワークサーバ上でBroadWorksサービスを再起動できます。再起動中は、既存のコールは中断されませんが、一部のサービスが一時的に使用できなくなる可能性があります。Cisco BroadWorksネットワークサーバのメモリ使用率を監視する方法の詳細は、『Cisco BroadWorksメンテナンスガイド』のセクション19「Cisco BroadWorksシステムの監視」を参照してください。

Cisco BroadWorksネットワークサーバの割り当てメモリを手動で解放する

この脆弱性の不正利用に成功し、DoS状態に達すると、BroadWorksネットワークサーバが応答しなくなる可能性があります。この場合、restartbwコマンドを使用して割り当てられたメモリを手動で解放し、ネットワークサーバ上のBroadWorksサービスを再起動することができます。詳細は、『Cisco BroadWorksメンテナンスガイド』のセクション7.7「Restart Server」およびセクション21.18「restartbw」を参照してください。

この操作により、システムが一定期間使用できなくなる可能性があるため、非冗長環境では注意して使用する必要があります。

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お

客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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完全なアップグレード ソリューション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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

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。

Cisco BroadWorksリリース	First Fixed Release（修正された最初のリリース）
リリース非依存(RI)[1]	RI.2024.11

1. Cisco BroadWorksのリリース25以降、すべてのサーバタイプはリリースに依存せず、日付ベー

スのリリース命名規則に従います。詳細については、 BroadWorks Release Independent Support Policyを参照してください。

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された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-bw-sip-dos-mSySbrmt

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	2025年1月22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。