Cisco BroadWorks CommPilotアプリケーションソフトウェアの脆弱性

Medium	**アドバイザリーID :** cisco-sa-broadworks-dJ9JT67N **初公開日 :** 2021-09-08 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.5 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvz32610 CSCvz32611	CVE-2021-34786 CVE-2021-34785

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 CommPilot Application Softwareの複数の脆弱性により、認証されたリモートの攻撃者が任意のユーザアカウントを削除したり、該当システムで権限を昇格させたりできる可能性があります。

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。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-dJ9JT67N

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性は、Webベース管理インターフェイスを通じて読み取り専用システム管理者ロールのアクセスを制限するユーザアクセスコントロールを実装した場合、修正済みリリースよりも前のCisco BroadWorks CommPilotアプリケーションソフトウェアリリースに影響しました。

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、この公開時点で脆弱性が存在していたシスコソフトウェアリリースに関する情報を確認してください。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工クスプロイトするために、他の脆弱性を工クスプロイトする必要はありません。また、いずれかの脆弱性の影響を受ける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-2021-34785：Cisco BroadWorks CommPilotアプリケーションソフトウェアの特権昇格の脆弱性

Cisco BroadWorks CommPilot Application SoftwareのWebベース管理インターフェイスの脆弱性により、認証されたリモート攻撃者が昇格された権限を取得できる可能性があります。

この脆弱性は、影響を受けるアプリケーションの操作に関する不適切な認証チェックに起因します。読み取り専用のシステム管理者権限を持つ攻撃者は、巧妙に細工された要求をアプリケーション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、攻撃者は既存のシステム管理者アカウントを変更し、対象アカウントの権限を引き受け、権限昇格を行う可能性があります。

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：CSCvz32611
CVE ID：CVE-2021-34785
セキュリティへの影響の評価（SIR）：中
CVSS ベーススコア：6.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H

CVE-2021-34786：Cisco BroadWorks CommPilotアプリケーションソフトウェアアカウント削除の脆弱性

Cisco BroadWorks CommPilot Application SoftwareのWebベース管理インターフェイスの脆弱性により、認証されたリモート攻撃者が任意のユーザアカウントを削除する可能性があります。

この脆弱性は、影響を受けるアプリケーションの操作に関する不適切な認証チェックに起因します。読み取り専用のシステム管理者権限を持つ攻撃者は、巧妙に細工された要求をアプリケーション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、攻撃者はターゲットアプリケーションから任意のユーザアカウントを削除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：CSCvz32610
CVE ID：CVE-2021-34786
セキュリティへの影響の評価（SIR）：中
CVSS ベーススコア：4.9
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/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

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

発行時点では、次の表のリリース情報が正確でした。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たシスコソフトウェアリリースが一覧表示されます。中央の列は、これらの脆弱性に対するパッチがリリースされたかどうか、および関連するベースソフトウェアのリリース番号を示します。右側の列には、使用可能なパッチのファイル名がリストされます。

Cisco BroadWorks CommPilotアプリケーションソフトウェアリリース	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.	—
21.0	計画なし.	—
22.0	22.0.2021.09	AP.xsp.22.0.1123.ap380970 AP.as.22.0.1123.ap380970
23.0	23.0.2021.09	AP.xsp.23.0.1075.ap380970 AP.as.23.0.1075.ap380970
24.0	24.0.2021.09	AP.as.24.0.944.ap380970

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と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Eslam Aklに感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-dJ9JT67N

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	—	最終版	2021年9月8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。