シスコの音声オペレーティング システムをベースとした製品に不正アクセスの脆弱性

Critical

アドバイザリーID : cisco-sa-20171115-vos

初公開日 : 2017-11-15 16:00

バージョン 1.0 : Final

CVSSスコア : 9.8

回避策 : No workarounds available

Cisco バグ ID : CSCvg68797 CSCvg55112 CSCvg55145 CSCvg22923 CSCvg64456 CSCvg58619 CSCvg64453 CSCvg64464 CSCvg64475 CSCvg55128

CVE-2017-12337

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

シスコの音声オペレーティング システム ソフトウェア プラットフォームをベースとしたシスコ コラボレーション製品には、アップグレード機能に脆弱性があり、認証を受けていないリモートの攻撃者が、該当するデバイスに不正アクセスしたり、権限を昇格させた上でアクセスしたりする可能性があります。

本脆弱性は、該当するデバイスで更新アップグレードを行うか、Prime Collaboration Deployment（PCD）での移行を行う際に顕在化します。 リフレッシュ アップグレードか PCD 移行が正常に完了するとき、エンジニアリング フラグはイネーブルになっている残り、既知 パスワードでデバイスに *ルートアクセス*を許可する可能性があります。

その後、脆弱なデバイスが標準のアップグレード手法でエンジニアリング スペシャル リリース、サービス アップデート、該当製品の新しいメジャー リリースにアップグレードされることで、本脆弱性が修正されます。

注: エンジニアリング スペシャル リリースが COP ファイルとしてインストールされる場合は、標準のアップグレード手法をとる場合とは異なり、本脆弱性は修正されません。

脆弱 な状態にある間、SFTP 上の影響を受けたデバイスにアクセスできる攻撃者はデバイスに *ル*

ートアクセスを得る可能性があります。 アクセスされると、攻撃者によって該当するシステムが完全に侵害される可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-vos

該当製品

脆弱性のある製品

本脆弱性は、次のシスコの音声オペレーティング システム（VOS）をベースとした製品が、更新アップグレード（RU）の手法でアップグレードされた場合、または Prime Collaboration Deployment（PCD）を通じて移行された場合に、影響を及ぼします。

- Cisco Unified Communications Manager（UCM）
- Cisco Unified Communication Manager Session Management Edition（SME）
- Cisco Emergency Responder
- Cisco Unity Connection
- Cisco Unified Communications Manager IM and Presence Service（IM&P： 旧リリース名称 Cisco Unified Presence）
- Cisco Prime License Manager
- Cisco Hosted Collaboration Mediation Fulfillment
- Cisco Unified Contact Center Express（UCCx）
- Cisco SocialMiner
- Cisco Unified Intelligence Center（UIC）
- Cisco Finesse
- Cisco MediaSense

PCD での移行が関係するのは、Cisco UCM、SME、IM&P のみです。

アップグレード手法または移行手法の判別

上述の脆弱な製品のリストに示された Cisco VOS をベースとした製品は、更新アップグレードまたは PCD での移行が行われる場合に、本脆弱性の影響を受けます。 なお、VOS をベースとした製品は、基盤となるオペレーティング システムを新しいメジャー リリースにアップグレードする際にも、更新アップグレードの必要がある点に注意してください。

VOS ベースの製品がエンジニアリング特派員にアップグレードされた規格であった場合場合アップデートを保守すれば、基礎オペレーティング システムに主要なアップグレードを必要としない影響を受けた製品の新しいメジャーリリースはその標準アップグレード操作によって、この脆弱性 remediated。

リフレッシュ アップグレード 方式 確認

製品がリフレッシュ アップグレード 方式によって脆弱性--にさらされたかどうか確かめるために、 *system-history.log* ファイルを表示するために CLI で次のコマンドを発行して下さい:

```
admin: file view install system-history.log
```

次の例は *system-history.log* ファイルでリフレッシュ Upgrade エントリを示したものです:

```
admin: file view install system-history.log
```

次の例は *system-history.log* ファイルで標準アップグレード エントリを示したものです:

```
admin: file view install system-history.log
```

PCD 移行 メソッド 確認

製品が PCD 移行 メソッドによってこの脆弱性--にさらされたかどうか確かめるために、 *install.log* ファイルを表示するために CLI で次のコマンドを発行して下さい:

```
admin: file view install install.log
```

次の例は *install.log* ファイルで PCD 移行 Log エントリを示したものです:

```
admin: file view install install.log
```

次の例は *install.log* ファイルで正常で新しいインストール Log エントリを示したものです:

```
admin: file view install install.log
```

新しいメジャーリリースにアップグレードされる基礎オペレーティング システム

VOS をベースとした製品では、基盤となるオペレーティング システムを新しいメジャー リリースにアップグレードする際にも、更新アップグレードが行われます。

次の例では、影響を受ける製品のメジャー リリースに関連するオペレーティング システムのメジャー リリースが示されています。

Cisco UCM、Cisco Unity Connection、Cisco Unified Presence Server/Cisco IM&P メジャー リリース	オペレーティング システム メジャーリリース
8.6	RHEL 5 Update 5

9.x	RHEL 5 Update 7
10.x	RHEL 6 Update 2
11.x	RHEL 6 Update 5
12.x	CentOS 6 Update 6

RHEL 6 から CentOS 6 へのアップグレードについては、オペレーティング システムのメジャー リリースの変更とはみなせないため、これらのオペレーティング システム リリース間での製品アップデートには、標準アップグレードの手法が使われます。

Prime Collaboration 配備クラスタ 移行

Prime Collaboration Deployment は、さまざまな Cisco Unified Communications アプリケーションの管理に役立つように設計されたフリーのアプリケーションです。 PCD での移行におけるクラスタ タスクは、次のシスコ製品の特定のクラスタ移行先バージョンでのみサポートされています。

- UCM の移行先バージョン 10.x、11.0(1)、11.5(x)、12.0(1)
- IM&P の移行先バージョン 10.x、11.0(1)、11.5(x)、12.0(1)

特定のアップグレード手法や移行手法の情報については、製品マニュアルを参照してください。

シスコ ユニファイド プラットフォームの現在のソフトウェア リリースの判別

次のシスコ製品では、シスコ ユニファイド プラットフォームを実行しています。

- Unified Communications Manager
- Unified Communications Manager Session Management Edition
- Emergency Responder
- Unity Connection
- Unified Communications Manager IM and Presence Service
- Prime License Manager
- Hosted Collaboration Mediation Fulfillment

どの Cisco を VOS ベースの製品ソフトウェア リリースが Cisco Unified プラットフォームで経営しているか判別するために、管理者は CLI で **show version アクティブな**コマンドを発行できます。

次の例では、ソフトウェア リリースが 11.5.1.10000-86 になっています。

```
ciscocm: show version active
Active Master Version: 11.5.1.10000-86
```

管理者は、ユーザ インターフェイスを使用して、Cisco VOS をベースとしたどの製品のソフトウェア リリースが実行されているかを確認できます。

1. Web ベースのインターフェイスにログインします。
2. **Help メニューを**クリックして下さい
3. システムソフトウェアリリースを表示するために『About』 をクリック して下さい

シスコ コンタクト センター プラットフォームの現在のソフトウェア リリースの判別

次のシスコ製品では、シスコ コンタクト センター プラットフォームを実行しています。

- Unified Contact Center Express
- SocialMiner
- Unified Intelligence Center
- Finesse
- MediaSense

どの Cisco を VOS ベースの製品ソフトウェア リリースがコンタクトセンター プラットフォームで経営しているか判別するために、管理者は CLI で **show version アクティブな**コマンドを発行できます。

次の例では、ソフトウェア リリースが 11.5.1.10000-86 になっています。

```
admin: show version active
Active Master Version: 11.5.1.10000-86
```

管理者は、ユーザ インターフェイスを使用して、シスコ コンタクト センター プラットフォームをベースとしたどの製品のソフトウェア リリースが実行されているかを確認できます。

1. Contact Center Express サーバにログインします。
2. Cisco Unified Communications オペレーティング システムの管理ウィンドウに移動します。
3. **示します > ソフトウェア**選択して下さい

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

シスコは、この脆弱性が以下の製品には影響を与えないことを確認しました。

- Cisco Identity Service（IdS）11.5 および 11.6

- Cisco Prime Collaboration Deployment
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Assurance
- Cisco Virtualized Voice Browser

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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。

ソフトウェアのアップグレードを検討する際には、 Cisco Security Advisories and Alerts 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 に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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。

修正済みリリースおよびソフトウェア ダウンロード

Cisco Unified Communications Manager - Cisco バグ ID CSCvg22923

Cisco Unified Communications Manager ソフトウェアは Cisco.com の Software Center から **製品 > ユニファイド コミュニケーション > 呼制御 > Unified Communications Manager (CallManager)** へのによってナビゲート ダウンロードすることができます。

Cisco Unified Communications Manager メジャー リリース	このアドバイザリのための治療ソリューション
8.6	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
~ 9.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
9.1	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行
10.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
10.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
12.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用

Cisco Unified Communications Manager Session Management Edition - Cisco バグ ID CSCvg22923

Cisco Unified Communications Manager Session Management Edition （SME）ソフトウェアは Cisco.com の Software Center から **製品 > ユニファイド コミュニケーション > 呼制御 > Unified Communications Manager Session Management Edition > Unified Communications Manager/Cisco Unity Connection ユーティリティ**へのによってナビゲート ダウンロードすることができます。

Cisco Unified Communications Manager SME メジャーリリース	このアドバイザリのための治療ソリューション
8.6	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
~ 9.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
9.1	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
10.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
10.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
12.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-

	v1.0.k3.cop.sgn を適用

Cisco Emergency Responder - Cisco バグ ID CSCvg55112

Cisco Emergency Responder ソフトウェアは Cisco.com の Software Center から **製品 > ユニファイド コミュニケーション > テレフォニー エクステンション > Emergency Responder** へのによってナビゲート ダウンロードすることができます。

Cisco Emergency Responder メジャーリリース	このアドバイザリのための治療ソリューション
8.6	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
8.7	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
~ 9.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
10.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
10.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
12.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。

Cisco Unity Connection - Cisco バグ ID CSCvg55128

Cisco Unity Connection ソフトウェアは Cisco.com の Software Center から **製品 > ユニファイド コミュニケーション > ユニファイド コミュニケーション アプリケーション > メッセージング > Unity Connection** へのによってナビゲート ダウンロードすることができます。

Cisco Unity Connection メジャーリリース	このアドバイザリのための治療ソリューション
8.6	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
~ 9.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
9.1	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
10.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
10.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
12.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。

Cisco Unified Communications Manager IM および存在サービス- Cisco バグ ID CSCvg22923

Cisco Unified Communications Manager は Cisco.com の Software Center から **製品 > ユニファイド コミュニケーション > ユニファイド コミュニケーション アプリケーション > プレゼンス ソフトウェア > Unified Communications Manager IM & プレゼンスサービス**へのによって IM および存在サービス ソフトウェア ナビゲート ダウンロードすることができます。

Cisco Unified IM および存在サービス メジャーリリース	このアドバイザリのための治療ソリューション
8.6 (Unified Presence)	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
~ 9.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
9.1	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
10.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
10.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
12.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。

Cisco Prime License Manager - Cisco バグ ID CSCvg58619

Cisco Prime License Manager ソフトウェアは Cisco.com の Software Center から **製品 > ユニフ**

ァイド コミュニケーション > ユニファイド コミュニケーション管理 > Prime License Manager > Prime License Manager ソフトウェア アップデートへのによってナビゲート ダウンロードすることができます。

Cisco Prime License Manager メジャーリリース	このアドバイザリのための治療ソリューション
9.0 (Enterprise License Manager)	脆弱性なし
10.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
10.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.0	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。

Cisco Hosted Collaboration Mediation 達成- Cisco バグ ID CSCvg68797

Cisco Hosted Collaboration Mediation 達成ソフトウェアは Cisco.com の Software Center から **製品 > ユニファイド コミュニケーション > 呼制御 > ホステッド コラボレーション > Hosted Collaboration ソリューション (HCS)** へのによってナビゲート ダウンロードすることができます。

Cisco Hosted Collaboration ソリューション メジャーリリース	このアドバイザリのための治療ソリューション
9.2	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
9.2(1)	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn

	を適用。またはサービス アップデートを実行。
9.2(1)SU1	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.cop.sgn を適用。またはサービス アップデートを実行。
10.0(1)	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
10.1(1)	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
10.1(2)	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
10.6(1)	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用。またはサービス アップデートを実行。
11.5	脆弱性あり; COP ファイル ciscocm.CSCvg22923-v1.2.k3.cop.sgn を適用

Cisco Unified Contact Center Express - Cisco バグ ID CSCvg55145

Cisco Unified Contact Center Express ソフトウェアは Cisco.com の Software Center から **製品 > カスタマー コラボレーション > コンタクト センター ソリューション > Unified Contact Center Express** へのによってナビゲート ダウンロードすることができます。

Cisco Unified Contact Center Express メジャー リリース	このアドバイザリのための治療ソリューション
8.5(1)	脆弱性なし
9.0(1)	脆弱性なし
9.0(2)	脆弱性なし
10.0(1)	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービス アップデートを実行。

10.5(1)	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
10.6(1)	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
11.0(1)	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
11.5(1)	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
11.6(1)	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用

Cisco SocialMiner - Cisco バグ ID CSCvg64453

Cisco SocialMiner ソフトウェアは Cisco.com の Software Center から **製品 > カスタマー コラボレーション > コンタクト センター ソリューションのオプション > SocialMiner > SocialMiner ソフトウェア**へのによってナビゲート ダウンロードすることができます。

Cisco SocialMiner メジャーリリース	このアドバイザリのための治療ソリューション
8.5	脆弱性なし
~ 9.0	脆弱性なし
10.0	脆弱性なし
10.5	脆弱性なし
10.6	脆弱性あり; COP ファイル ciscosm-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
11.0	脆弱性あり; COP ファイル ciscosm-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用

ライブ データの Cisco Unified Intelligence Center および Cisco Unified Intelligence Center - Cisco

バグ ID CSCvg64464

Cisco Unified Intelligence Center ソフトウェアは Cisco.com の Software Center から **製品 > カスタマー コラボレーション > コンタクト センター ソリューションのオプション > Unified Intelligence Center > Unified Intelligence Center ソフトウェア**へのによってナビゲート ダウンロードすることができます。

Cisco Unified Intelligence Center メジャーリリース	このアドバイザリのための治療ソリューション
8.5	脆弱性なし
~ 9.0	脆弱性なし
9.1	脆弱性なし
10.0	脆弱性なし
10.5	脆弱性なし
11.0	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
11.5	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
11.6	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用

Cisco Finesse - Cisco バグ ID CSCvg64475

Cisco Finesse ソフトウェアは Cisco.com の Software Center から **製品 > カスタマー コラボレーション > コンタクト センター ソリューションのオプション > Finesse > Finesse ソフトウェア**へのによってナビゲート ダウンロードすることができます。

Cisco Finesse メジャーリリース	このアドバイザリのための治療ソリューション
8.5	脆弱性なし
~ 9.0	脆弱性なし
10.0	脆弱性なし
10.5	脆弱性なし
11.0	脆弱性あり; COP ファイル ucos-

	psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
11.5	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
11.6	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用

Cisco MediaSense - Cisco バグ ID CSCvg64456

Cisco MediaSense ソフトウェアは Cisco.com の Software Center から **製品 > カスタマー コラボレーション > コンタクト センター ソリューションのオプション > MediaSense > MediaSense ソフトウェア**へのによってナビゲート ダウンロードすることができます。

Cisco MediaSense メジャーリリース	このアドバイザリのための治療ソリューション
8.5	脆弱性なし
～ 9.0	脆弱性なし
10.0	脆弱性なし
10.5	脆弱性なし
11.0	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用。またはサービスアップデートを実行。
11.5	脆弱性あり; COP ファイル ucos-psirt-root-access-CSCvg55145-k3-1.1.cop.sgn を適用

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やその公表を確認していません。

出典

本脆弱性は、State Farm Penetration Testing Team の Quentin Rhoads-Herrera と Rich Mirch によりシスコに報告されました。両人に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-vos

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 11 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。