複数のシスコ製品におけるディスク使用率による Denial of Service（DoS）の脆弱性

High

アドバイザリーID： cisco-sa-20180606-diskdos

初公開日： 2018-06-06 16:00

最終更新日： 2018-07-02 14:32

バージョン 1.1： Final

CVSSスコア： 8.6

回避策： No workarounds available

Cisco バグ ID： CSCvf64322 CSCvi31762 CSCvf64332 CSCvi31738 CSCvi31807 CSCvi31818 CSCvi29538 CSCvi29546 CSCvi29544 CSCvd10872 CSCvi29556 CSCvi29543 CSCvi31741 CSCvi29571 CSCvi31823

CVE-2017-6779

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 コラボレーション製品の特定のシステム ログ ファイルのローカル ファイル管理における脆弱性が、複数のシスコ製品に影響を与えます。この脆弱性により、認証されていないリモートの攻撃者がディスクの高使用率を引き起こし、結果として Denial of Service（DoS）状態となる場合があります。

この脆弱性は、特定のシステム ログ ファイルに最大サイズの制限がないことに起因します。 このため、アプライアンスで利用可能なディスク容量の大部分をファイルが消費することが可能です。 攻撃者は、巧妙に細工されたリモート接続要求をアプライアン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。 不正利用に成功すると、攻撃者はシステム ログ ファイルがディスク領域のほとんどを消費するようにログ ファイルのサイズを増大させることが可能になる場合があります。 使用可能なディスク領域の不足によって DoS 状態になり、アプリケーション機能が異常動作し、不安定になります。

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-20180606-diskdos

該当製品

脆弱性のある製品

この脆弱性は、次の Cisco 音声オペレーティング システム（VOS）ベースの製品に影響を及ぼします。

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

この脆弱性は、以下のシスコ製品にも影響します。

- Prime Collaboration Assurance
- Prime Collaboration Provisioning

CLI から現在のソフトウェア リリースを確認する

プラットフォームで実行しているソフトウェア リリースは、管理者が CLI から **show version active** コマンドを実行することで確認できます。

次の例では、ソフトウェア リリースは **11.5.1.10000-86** です。

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

Cisco Unified Contact Center プラットフォームの現在のソフトウェア リリースの確認

管理者は UI を使用して、実行されているソフトウェア リリースを確認できます。

1. Web ベースのインターフェイスにログインします。
2. [ヘルプ（Help）] > [バージョン情報（About）] を選択して、システム ソフトウェア リリースを確認します。

管理者は UI 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. [表示（Show）] > [ソフトウェア（Software）] を選択します。

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。]

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Identity Service（IdS）11.5 および 11.6
- Prime Collaboration Deployment

セキュリティ侵害の痕跡

この脆弱性が不正利用されると、次のエラーがデバイス ログに記録されます。

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

管理者は、このエラーを確認した場合、この脆弱性の不正利用によってデバイスが侵害されていないかどうかを確認するために Cisco Technical Assistance Center（TAC）に連絡してください。

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。

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。

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。
https://www.cisco.com/c/en/us/support/web/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

Emergency Responder： CSCvf64322

Cisco Emergency Responder ソフトウェアは、Cisco.com のSoftware Center からダウンロードできます。**[製品（Products）] > [Unified Communications] > [テレフォニー拡張（Telephony Extensions）] > [Emergency Responder]** の順に移動してください。

Emergency Responder リリース	この脆弱性に対する最初の修正リリース
10.5 より前	脆弱性あり; 10.5(1a) への移行が必要
10.5	10.5(1a)（今後リリース予定）[1]
11.0	脆弱性あり; 11.5(4) への移行が必要
11.5	11.5(4)
12.0	12.0SU1

[1] COP ファイル *ciscocm.cer_CSCvf64322.cop.sgn* は、cisco.com の Software Center から入手で

きます。

Finesse： CSCvi29556

Cisco Finesse ソフトウェアは、Cisco.com の Software Center からダウンロードできます。**[製品（Products）] > [カスタマーコラボレーション（Customer Collaboration）] > [コンタクトセンターソリューション用オプション（Options for Contact Center Solutions）] > [Finesse] > [Finesseソフトウェア（Finesse Software）]** の順に移動してください。

Finesse リリース	この脆弱性に対する最初の修正リリース
11.6 より前	脆弱性あり; 11.6(1) への移行が必要
11.6	11.6(1)

Hosted Collaboration Mediation Fulfillment： CSCvi31738

Cisco Hosted Collaboration Mediation Fulfillment ソフトウェアは、Cisco.com の Software Center からダウンロードできます。 **[製品（Products）] > [Unified Communications] > [コール制御（Call Control）] > [Hosted Collaboration] > [Hosted Collaboration Solution (HCS)]** の順に移動してください。

Hosted Collaboration Mediation Fulfillment リリース	この脆弱性に対する最初の修正リリース
11.5 より前	脆弱性あり; 11.5(3) への移行が必要
11.5	11.5(3)

MediaSense： CSCvi29546

Cisco MediaSense ソフトウェアは、Cisco.com の Software Center からダウンロードできます。**[製品（Products）] > [カスタマーコラボレーション（Customer Collaboration）] > [コンタクトセンターソリューション用オプション（Options for Contact Center Solutions）] > [MediaSense] > [MediaSenseソフトウェア（MediaSense Software）]** の順に移動してください。

MediaSense リリース	この脆弱性に対する最初の修正リリース
11.5 より前	脆弱性あり; 11.5SU2 への移行が必要
11.5	11.5SU2

Prime Collaboration Assurance： CSCvi31818

Prime Collaboration Assurance ソフトウェアは、Cisco.com の Software Center からダウンロードできます。**[製品（Products）] > [クラウドおよびシステム管理（Cloud and Systems Management）] > [コラボレーションおよびユニファイドコミュニケーション管理（Collaboration and Unified Communications Management）] > [Prime Collaboration]** の順に移動してください。

Prime Collaboration Assurance リリース	この脆弱性に対する最初の修正リリース

11.6 より前	脆弱性あり; 11.6 ES16 への移行が必要
11.6	11.6 ES16
12.1	12.1 ES2

Prime Collaboration プロビジョニング： CSCvi31741

Prime Collaboration プロビジョニング ソフトウェアは、Cisco.com の Software Center からダウンロードできます。**[製品（Products）] > [クラウドおよびシステム管理（Cloud and Systems Management）] > [コラボレーションおよびユニファイドコミュニケーション管理（Collaboration and Unified Communications Management）] > [Prime Collaboration]** の順に移動してください。

Prime Collaboration プロビジョニング リリース	この脆弱性に対する最初の修正リリース
12.5 より前	脆弱性あり; 12.5 への移行が必要
12.5	12.5

Prime License Manager： CSCvi31807

Cisco Prime License Manager ソフトウェアは、Cisco.com の Software Center からダウンロードできます。 **[製品（Products）] > [Unified Communications] > [Unified Communications Management] > [Prime License Manager] > [Prime License Managerソフトウェアアップデート（Prime License Manager Software Updates）]** の順に移動してください。

Prime License Manager リリース	この脆弱性に対する最初の修正リリース
10.5 より前	脆弱性あり; plm_10_5_2 への移行する- 10.5.2.13001-1[1]
10.5	plm_10_5_2 - 10.5.2.13001-1
11.0	脆弱性あり; 11.5(1)SU5 への移行が必要
11.5	11.5(1)SU5

SocialMiner： CSCvi29544

Cisco SocialMiner ソフトウェアは、Cisco.com の Software Center からダウンロードできます。**[製品（Products）] > [カスタマーコラボレーション（Customer Collaboration）] > [コンタクトセンターソリューション用オプション（Options for Contact Center Solutions）] > [SocialMiner] > [SocialMinerソフトウェア（SocialMiner Software）]** の順に移動してください。

SocialMiner リリース	この脆弱性に対する最初の修正リリース
11.6 より前	脆弱性あり; 11.6.1 への移行が必要
11.6	11.6.1

Unified Communications Manager および Unified Communication Manager Session Management Edition： CSCvd10872

Cisco Unified Communications Manager ソフトウェアは、Cisco.com の Software Center からダ

ウンロードできます。**[製品（Products）] > [Unified Communications] > [コール制御（Call Control）] > [Unified Communications Manager (CallManager)]** の順に移動してください。

Unified Communications Manager リリース	この脆弱性に対する最初の修正リリース
10.0 より前	脆弱性あり; 10.5(2)SU5 以降への移行が必要
10.0	脆弱性あり; 10.5(2)SU5 以降への移行が必要
10.5	10.5(2)SU5
11.0	11.0(1a)SU4
11.5	11.5(1)SU3
12.0	脆弱性なし

Unified Communications Manager IM and Presence Service： CSCvi29543

Cisco Unified Communications Manager IM and Presence Service ソフトウェアは、Cisco.com の Software Center からダウンロードできます。**[製品（Products）] > [Unified Communications] > [Unified Communicationsアプリケーション（Unified Communications Applications）] > [プレゼンスソフトウェア（Presence Software）] > [Unified Communications Manager IM & Presence Service]** の順に移動してください。

Unified Communications Manager IM and Presence Service リリース	この脆弱性に対する最初の修正リリース
10.5 より前	脆弱性あり; 10.5.2 SU4 への移行が必要
10.5	10.5.2SU4
11.0	脆弱性あり; 11.5(1)SU4 への移行が必要
11.5	11.5(1)SU4

Unified Contact Center Express： CSCvi29538

Cisco Unified Contact Center Express ソフトウェアは、Cisco.com の Software Center からダウンロードできます。 **[製品（Products）] > [カスタマーコラボレーション（Customer Collaboration）] > [コンタクトセンターソリューション用オプション（Options for Contact Center Solutions）] > [Unified IP Interactive Voice Response (IVR)]** の順に移動してください。

Unified Contact Center Express リリース	この脆弱性に対する最初の修正リリース
11.6 より前	脆弱性あり; 11.6(1) への移行が必要
11.6	11.6(1)

Unified Intelligence Center： CSCvi29571

Cisco Unified Intelligence Center ソフトウェアは、Cisco.com の Software Center からダウンロードできます。**[製品（Products）] > [カスタマーコラボレーション（Customer Collaboration）] > [コンタクトセンターソリューション用オプション（Options for Contact Center Solutions）] >**

[Unified Intelligence Center] > [Unified Intelligence Centerソフトウェア（Unified Intelligence Center Software）] の順に移動してください。

Unified Intelligence Center リリース	この脆弱性に対する最初の修正リリース
11.6 より前	脆弱性あり; 11(6).1 への移行が必要
11.6	11.6(1)

Unity Connection： CSCvf64332

Cisco Unity Connection ソフトウェアは、Cisco.com の Software Center からダウンロードできます。**[製品（Products）] > [Unified Communications] > [Unified Communicationsアプリケーション（Unified Communications Applications）] > [メッセージング（Messaging）] > [Unity Connection]** の順に移動してください。

Unity Connection リリース	この脆弱性に対する最初の修正リリース
10.5 より前	脆弱性あり; 10.5SU5 への移行が必要
10.5	10.5SU5
11.0	脆弱性あり; 11.5(1)SU3 への移行が必要
11.5	11.5.1SU3
12.0	脆弱性なし

Virtualized Voice Browser： CSCvi31823

Cisco Virtualized Voice Browser ソフトウェアは、Cisco.com の Software Center からダウンロードできます。**[製品（Products）] > [カスタマーコラボレーション（Customer Collaboration）] > [コンタクトセンターソリューション用オプション（Options for Contact Center Solutions）] > [Virtualized Voice Browser]** の順に移動してください。

Virtualized Voice Browser リリース	この脆弱性に対する最初の修正リリース
11.6 より前	脆弱性あり; 11.6(1) への移行が必要
11.6	11.6(1)

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

この脆弱性は、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-diskdos

改訂履歴

Version	Description	Section	Status	日付
1.1	Prime License Manager の修正済みリリースの表を更新。	修正済みソフトウェア	Final	2018 年 7 月 2 日
1.0	初回公開リリース		Final	2018 年 6 月 6 日

利用規約