

Cisco Digital Media Managerの複数の脆弱性

Critical	アドバイザーID : cisco-sa-20100303-dmm	CVE-2010-0571
	初公開日 : 2010-03-03 16:00	CVE-2010-0572
	バージョン 1.0 : Final	CVE-2010-0570
	CVSSスコア : 10.0	
	回避策 : No Workarounds available	
	Cisco バグ ID :	

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 Digital Media Manager(DMM)には複数の脆弱性が存在します。このセキュリティアドバイザリでは、次の脆弱性の詳細について説明します。

- デフォルト クレデンシャル
- 特権昇格の脆弱性
- 情報漏洩の脆弱性

これらの脆弱性は相互に関連していません。

これらの脆弱性を軽減できる回避策はありません。

このアドバイザリは、

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100303-dmm> で公開されています。

注 : このアドバイザリは、Cisco Digital Media Playerに影響を与える脆弱性情報開示アドバイザリと同時にリリースされます。このアドバイザリは、

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100303-dmp> で公開されています。

該当製品

脆弱性のある製品

以下は、本アドバイザリに記載されている各脆弱性の影響を受ける製品のリストです。

デフォルト クレデンシャル

Cisco DMMバージョン5.0.xおよび5.1.xは、この脆弱性の影響を受けます。Cisco DMMバージョン4.xには脆弱性はありません。

特権昇格の脆弱性

Cisco DMMバージョン5.0.xおよび5.1.xは、この脆弱性の影響を受けます。Cisco DMMバージョン4.xには脆弱性はありません。

情報漏洩の脆弱性

5.2より前のすべてのCisco DMMリリースは、この脆弱性の影響を受けます。

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。

詳細

Cisco DMMは、Cisco Digital Signs、Cisco Cast、およびCisco Show and Shareのデジタルメディアを管理、スケジュール、および公開するために使用されます。このセキュリティアドバイザリでは、Cisco DMMの複数の個別の脆弱性について説明します。これらの脆弱性は相互に関連していません。

デフォルト クレデンシャル

5.2よりも前のバージョンのCisco DMMには、デフォルトのクレデンシャルが設定されており、インストールされているWebアプリケーション（設定、ステータス、展開など）を攻撃者が完全に制御できる可能性があります。

この脆弱性は、Cisco Bug ID [CSCta03378](#)(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2010-0570が割り当てられています。

特権昇格の脆弱性

Cisco DMMバージョン5.0.xおよび5.1.xには脆弱性が存在します。この脆弱性により、認証されたユーザが権限のないユーザによって設定を変更し、デバイスのフルアクセスを取得できる可能性があります。

この脆弱性は、Cisco Bug ID [CSCtc46008](#) (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2010-0571が割り当てられています。

情報漏洩の脆弱性

Cisco DMMは、Cisco Digital Media Playerの管理に使用できます。Cisco Digital Media PlayerはIPベースのエンドポイントで、高解像度のライブビデオやオンデマンドビデオ、モーショングラフィックス、Webページ、ダイナミックコンテンツをデジタルディスプレイで再生できます。

5.2よりも前のすべてのCisco DMMバージョンには脆弱性が存在します。この脆弱性により、認証されたものの不正なユーザが、エラーログメッセージおよびスタックトレース内のCisco Digital Media PlayerユーザクレデンシャルとLDAPクレデンシャル (設定されている場合) を表示できる可能性があります。

この脆弱性は、Cisco Bug ID CSCtc46050 (登録ユーザ専用) CSCtc53098(登録ユーザ専用)、CSCtc53024(登録ユーザ専用)に記載されています。

この脆弱性には、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2010-0572が割り当てられています。

回避策

これらの脆弱性を軽減できる回避策はありません。

修正済みソフトウェア

アップグレードを検討する場合は、<http://www.cisco.com/go/psirt> と後続のアドバイザリも参照して、問題の解決状況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機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center (TAC) または契約を結んで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。

このセキュリティアドバイザリに記載されているすべての脆弱性は、Cisco DMMバージョン5.2で修正されています。

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。

権限昇格と情報漏洩の脆弱性は、National Australia BankのSecurity Assuranceチームからシスコに報告されました。Cisco PSIRTは、研究者と協力してセキュリティの脆弱性に関する調査を行う機会を高く評価しており、製品レポートのレビューと支援を行う機会を歓迎しています。

デフォルトのクレデンシャルの脆弱性は、内部テスト中に発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100303-dmm>

改訂履歴

リビジョン 1.0	2010年3月3日	初回公開リリース
--------------	-----------	----------

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、単独の転載や意識を施した場合、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。