Cisco Security Advisory: Cisco Digital Media Manager Privilege Escalation Vulnerability

Advisory ID: cisco-sa-20120118-dmm

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120118-dmm

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。

Revision 1.0

For Public Release 2012 January 18 16:00 UTC (GMT)

目次

要約
該当製品
詳細
脆弱性スコア詳細
影響
ソフトウェア バージョンおよび修正
回避策
修正済みソフトウェアの入手
不正利用事例と公式発表
この通知のステータス : FINAL
情報配信
更新履歴
シスコ セキュリティ手順

要約

Cisco Digital Media Manager には、リモートの認証された攻撃者が権限を昇格し、該当システムに対する完全なアクセス権を取得できる可能性のある脆弱性が存在します。

Cisco Show and Share は、この脆弱性の直接の影響は受けませんが、 Cisco Show and Share の認証サービスは Cisco Digital Media Manager に依存しているため、攻撃者が Cisco Digital Media Manager の脆弱性を不正利用することにより、Cisco Show and Share に対する完全なアクセス権を取得する可能性があります。

シスコはこの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ました。

この脆弱性を軽減する対応策はありません。

このアドバイザリは次のリンクに掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120118-dmm

該当製品

脆弱性が存在する製品

次の表に、この脆弱性の影響を受ける Cisco Digital Media Manager のバージョンを示します。

Version	Affected
prior to 5.2	YES
5.2.1	YES
5.2.1.1	YES
5.2.2	YES
5.2.2.1	NO
5.2.3	YES
5.3	NO

注： バージョン 5.2 より前の Cisco Digital Media Manager はソフトウェア メンテナンスが終了しています。5.2 より前のバージョンを使用している場合は、サポートされている Cisco Digital Media Manager のバージョンへのアップグレードに関してシスコ サポート チームにお問い合わせください。

ソフトウェア バージョンを知る方法

アプライアンスで実行されている Cisco Digital Media Manager ソフトウェアのバージョンを確認するには、管理者は Cisco Digital Media Manager Web インターフェイスにアクセスします。ページ中央の [Digital Media Manager] の下に バージョン情報が記載されています。

または、Appliance Administration Interface（AAI）にログインして、メイン メニューにアクセスします。[Cisco Digital Media Manager] フィールドの横にソフトウェアのバージョンが記載されています。次の例は、バージョン 5.2.1 を実行している Digital Media Manager アプライアンスを示しています。

```
 Cisco Digital Media Manager Application Administration Interface
                                Main Menu
   IP: 192.168.0.1

   Cisco Digital Media Manager 5.2.1
   http://dmm.cisco.com:8080



        SHOW_INFO               Show system information.
        BACKUP_AND_RESTORE      Back up and restore.
        APPLIANCE_CONTROL       Configure advance options
        NETWORK_SETTINGS        Configure network parameters.
        DATE_TIME_SETTINGS      Configure date and time
        CERTIFICATE_MANAGEMENT  Manage all certificates in the system
```

< OK > <LOG OUT>

脆弱性が存在しない製品

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 Digital Media Manager（DMM）は、シスコのメディア ネットワーク ハードウェア、ソフトウェア、サービスを集中管理するために使用される Web ベースのプラットフォームです。 これを使用することで、Cisco Digital Signs、Cisco Cast、Cisco Show and Share の管理タスクをリモートで実行することが可能になります。

Cisco Digital Media Manager には、リモートの認証された攻撃者が権限を昇格し、該当システムに対する完全なアクセス権を取得できる可能性のある脆弱性が存在します。

この脆弱性は、非参照 URL（Unreferenced URL）の不適切な検証に起因し、権限のない攻撃者が管理リソースにアクセスして権限を昇格することが可能になることがあります。認証された攻撃者は、非参照の URL を該当システムに送信することで、この脆弱性を不正利用できる可能性があります。

Cisco Show and Share は、この脆弱性の直接の影響は受けませんが、 Cisco Show and Share の認証サービスは Cisco Digital Media Manager に依存しているため、攻撃者が Cisco Digital Media Manager の脆弱性を不正利用することにより、Cisco Show and Share に対する完全なアクセス権を取得する可能性があります。

この脆弱性は Cisco Digital Media Manager の管理ポートである TCP ポート 8443 で不正利用される可能性があります。

この脆弱性は、Cisco Bug ID CSCts63878（ 登録 ユーザのみ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-0329 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、個々のネット

ワークにおける脆弱性の影響度を導き出すことができます。

シスコは次の URL にて CVSS に関する FAQ を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを以下の URL にて提供しています。
http://tools.cisco.com/security/center/cvssCalculator.x

CSCts63878 - Digital Media Manager Privilege Escalation Vulnerability Calculate the environmental score of					
CVSS Base Score - **9.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、リモートの認証された攻撃者は権限を昇格し、該当システムに対する完全なアクセス権を取得できる可能性があります。

さらに、Cisco Show and Share の認証サービスは Cisco Digital Media Manager に依存しているため、 Cisco Digital Media Manager に対するこの脆弱性の不正利用に成功した場合、リモートの攻撃者は Cisco Show and Share に対する完全なアクセス権を取得する可能性があります。

ソフトウェア バージョンおよび修正

シスコはこの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ました。

次の表に、Cisco Digital Media Manager の各該当バージョンに対する修正を記載します。

Version	Remediation

5.2.1	Upgrade to 5.2.2.1
5.2.1.1	Upgrade to 5.2.2.1
5.2.2	Upgrade to 5.2.2.1
5.2.3	DMM523_PATCH-A.iso

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt および本アドバイザリ以降に公開のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

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。情報が不明確な場合は、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。

回避策

この脆弱性を軽減する対応策はありません。

ネットワーク内のシスコ デバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Intelligence』にて参照できます。
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20120118-dmm

修正済みソフトウェアの入手

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前にお客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

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、ご購入いただいたフィーチャ セットに対してのみとなります。お客様はソフトウェア 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利用することにより、
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html または
http://www.cisco.com/public/sw-center/sw-usingswc.shtml に記載されているシスコのソフトウェア ライセンス条件に同意したものと見なされます。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。大半のお客様は、 http://www.cisco.com にあるシスコの Web サイトの Software Center からアップグレードを入手できます。

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、本脆弱性に関する適切な処置について指示と支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品が多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

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 Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。TAC の連絡先は次のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このお知らせの URL をご用意ください。サービス契約をご利用でないお客様に対する無償アップグレードは、TAC 経由でご要求いただく必要があります。

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html を参照してください。

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とその公表は確認しておりません。

この脆弱性は Anthony Towry 氏からのお問い合わせへの対応の際に発見されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

本アドバイザリは、次のシスコのワールドワイド Web サイト上に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120118-dmm

ワールドワイド Web 以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものもシスコのワールドワイド Web サイトに掲載される予定です。しかしながら、前述のメーリング リストもしくはニュースグループに対し積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URL にて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2012-January-18	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、シスコ ワールドワイド Web サイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。このページには、シスコのセキュリティ通知に関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは http://www.cisco.com/go/psirtで確認することができます。