Cisco Security Advisory: Multiple Vulnerabilities in Cisco TelePresence Multipoint Switch

Advisory ID: cisco-sa-20110223-telepresence-ctms

http://www.cisco.com/warp/public/707/cisco-sa-20110223-telepresence-ctms.shtml

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 1.1

Last Updated 2011 March 9 2100 UTC (GMT)

For Public Release 2011 February 23 1600 UTC (GMT)

目次

要約

Cisco TelePresence Multipoint Switch には、複数の脆弱性が存在します。このアドバイザリは以下の脆弱性の要点について説明しています。

- Java Servlet による不正なアクセス
- 任意のファイルの不正なアップロード
- Cisco Discovery Protocol によるコードのリモート実行
- 不正な Servlet によるアクセス
- Java RMI のサービス拒否
- RTCP（Real-Time Transport Control Protocol）のサービス拒否

- RPC（XML-Remote Procedure Call）のサービス拒否

同じ問題を報告している、Cisco TelePresence に関するその他のアドバイザリ

Java Servlet による不正なアクセスの脆弱性は、Cisco TelePresence Multipoint Switch および Recording Server に影響します。各コンポーネントへの影響については、それぞれのアドバイザリで説明しています。これらの脆弱性の Cisco bug ID は、次のとおりです。

- Cisco TelePresence Multipoint Switch - CSCtf42008
- Cisco TelePresence Recording Server - CSCtf42005

任意のファイルが不正にアップロードされる脆弱性は、Cisco TelePresence Multipoint Switch および Recording Server に影響します。各コンポーネントへの影響については、それぞれのアドバイザリで説明しています。これらの脆弱性の Cisco bug ID は、次のとおりです。

- Cisco TelePresence Multipoint Switch - CSCth61065
- Cisco TelePresence Recording Server - CSCth85786

Cisco Discovery Protocol によるコードのリモート実行の脆弱性は、Cisco TelePresence エンドポイント デバイス、Cisco TelePresence Manager、Multipoint Switch、および Recording Server に影響します。各コンポーネントへの影響については、それぞれのアドバイザリで説明しています。これらの脆弱性の Cisco bug ID は、次のとおりです。

- Cisco TelePresence エンドポイント デバイス - CSCtd75754
- Cisco TelePresence Manager - CSCtd75761
- Cisco TelePresence Multipoint Switch - CSCtd75766
- Cisco TelePresence Recording Server - CSCtd75769

Java RMI のサービス拒否の脆弱性は、Cisco TelePresence Multipoint Switch および Recording Server に影響します。各コンポーネントへの影響については、それぞれのアドバイザリで説明しています。これらの問題に対する Cisco bug ID は次のとおりです。

- Cisco TelePresence Multipoint Switch - CSCtg35830
- Cisco TelePresence Recording Server - CSCtg35825

このアドバイザリは次のリンクに掲載されます。 http://www.cisco.com/warp/public/707/cisco-sa-20110223-telepresence-ctms.shtml

該当製品

これら脆弱性は Cisco TelePresence Multipoint Switch に影響を与えます。1.7.1 よりも前のすべての Cisco TelePresence システム ソフトウェアは、本アドバイザリで報告されている脆弱性の影響を受けます。

次の表に、脆弱性の影響を受けるソフトウェアの情報を示します。

Description	Cisco Bug ID	Affected Software Releases

Unauthenticated Java Servlet Access	CSCtf01253	1.0.x, 1.1.x, 1.5.x, 1.6.x
Unauthenticated Java Servlet Access	CSCtf42008	1.0.x, 1.1.x, 1.5.x, 1.6.x
Unauthenticated Arbitrary File Upload	CSCth61065	1.0.x, 1.1.x, 1.5.x, 1.6.x
Cisco Discovery Protocol Remote Code Execution	CSCtd75766	1.0.x, 1.1.x, 1.5.x, 1.6.x
Unauthorized Servlet Access	CSCtf97164	1.0.x, 1.1.x, 1.5.x, 1.6.x
Java RMI Denial of Service	CSCtg35825	1.0.x, 1.1.x, 1.5.x, 1.6.x
Real-Time Transport Control Protocol Denial of Service	CSCth60993	1.0.x, 1.1.x, 1.5.x, 1.6.x
XML-RPC Denial of Service	CSCtj44534	1.0.x, 1.1.x, 1.5.x, 1.6.x, 1.7.0, 1.7.1

脆弱性が存在する製品

該当するバージョンのソフトウェアが稼動している Cisco TelePresence Multipoint Switch デバイスは影響を受けます。

Cisco TelePresence Multipoint Switch で稼動しているソフトウェア バージョンを確認するには、デバイスへの SSH 接続を確立し、**show version active** および **show version inactive** コマンドを発行します。次のような結果が出力されます。

```
admin: show version active
Active Master Version: 1.7.0.0-471


Active Version Installed Software Options:
No Installed Software Options Found.

admin: show version inactive
Inactive Master Version: 1.6.1.0-336

Inactive Version Installed Software Options:
No Installed Software Options Found.
```

上記の例では、デバイスにはバージョン 1.6.1 および 1.7.0 がロードされており、現在アクティブなバージョンは 1.7.0 です。デバイスが影響を受けるのは、該当するソフトウェアのバージョンがアクティブになっている場合のみです。

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 TelePresence ソリューションは、遠く離れた場所にいる同僚や顧客、パートナーとの臨場感のある対面式のコミュニケーションやコラボレーションを、ネットワークを介して実現します。

このセキュリティ アドバイザリでは、Cisco TelePresence Multipoint Switch に存在する複数の相互に独立した脆弱性について説明しています。これら脆弱性は、互いに独立して存在します。

Java Servlet による不正なアクセス

Cisco TelePresence Multipoint Switch 内で Java Servlet フレームワークを介して配布される多くの Java Servlet によって、遠隔地にいる認証されていない攻撃者が、管理者権限を持つユーザのみしか実行できないアクションを実行する可能性があります。攻撃者は、該当するデバイスの TCP ポート 80、443、または 8080 に、巧妙に細工された要求を送信する必要があります。

攻撃者は、TCP 3 ウェイ ハンドシェイクを実行し、有効なセッションを確立しなければ、この脆弱性を悪用することはできません。

- CTMS - CSCtf42008（ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2011-0383 が割り当てられています。
- CTMS - CSCtf01253（ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2011-0384 が割り当てられています。

任意のファイルの不正なアップロード

任意のファイルがアップロードされる脆弱性は、Cisco TelePresence Multipoint Switch の管理用 Web インターフェイスに存在します。認証されていないリモートの攻撃者は、該当するデバイスに巧妙に細工された要求を送信することで、デバイスの任意の場所に自身が制御するコンテンツを配置することが可能になります。攻撃者は、該当するデバイスの TCP ポート 80 または 443 に、巧妙に細工された要求を送信する必要があります。

攻撃者は、TCP 3 ウェイ ハンドシェイクを実行し、有効なセッションを確立しなければ、この脆弱性を悪用することはできません。

- CTMS - CSCth61065（ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2011-0385 が割り当てられています。

Cisco Discovery Protocol によるコードのリモート実行

Cisco TelePresence Multipoint Switch デバイスには、リモートからコードを実行される脆弱性が存在します。認証されていない近接した攻撃者は、該当するシステムに悪意のある Cisco Discovery Protocol パケットを送信することで、この脆弱性を不正利用する可能性があります。悪意のあるパケットが解析されたとき、バッファ オーバーフローが引き起こされることがあります。

Cisco Discovery Protocol はデータリンク層（レイヤ 2）で動作するため、攻撃者は該当するデバイスにイーサネット フレームを直接送る方法を必要とします。これは、該当のデバイスがブリッジ型ネットワークに組み込まれている場合や、ネットワーク ハブのようなパーティション機能のないデバイスに接続されている場合に可能になります。

- CTMS - CSCtd75766（ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2011-

0379 が割り当てられています。

不正な Servlet によるアクセス

不正な Servlet によるアクセスの問題は、Cisco TelePresence Multipoint Switch デバイスの管理用 Web インターフェイスに存在します。この問題により、リモートの非特権アクセスを持つ認証された攻撃者が、該当するデバイスでサービス拒否（DoS）状態を引き起こす可能性があります。攻撃者は、該当するデバイスの TCP ポート 80 または 443 に、巧妙に細工された要求を送信する必要があります。

攻撃者は、TCP 3 ウェイ ハンドシェイクを実行し、有効なセッションを確立しなければ、この脆弱性を悪用することはできません。

- CTMS - CSCtf97164（ 登録ユーザのみ）として文書化され、CVE ID として CVE-2011-0387 が割り当てられています。

Java RMI のサービス拒否

サービス拒否の脆弱性は、Cisco TelePresence Multipoint Switch デバイスに存在します。これは、Java Servlet フレームワークの RMI インターフェイスへのアクセスが適切に制限されていないことに起因しています。リモートの認証されていない攻撃者が、巧妙に細工された要求を続けて送り、Servlet のホストでメモリ不足状態を引き起こす可能性があります。攻撃者は TCP ポート 8999 で、該当するデバイスと通信する必要があります。

攻撃者は、TCP 3 ウェイ ハンドシェイクを実行し、有効なセッションを確立しなければ、この脆弱性を悪用することはできません。

- CTMS - CSCtg35825（ 登録ユーザのみ）として文書化され、CVE ID として CVE-2011-0388 が割り当てられています。

RTCP のサービス拒否

RTCP（Real-Time Transport Control Protocol）のサービス拒否の脆弱性は、Cisco TelePresence Multipoint Switch デバイス内に存在します。認証されていないリモートの攻撃者が、悪意のある RTCP パケットをリスニング RTCP コントロール ポートに送信し、コール制御処理をクラッシュさせます。攻撃者は、コール セットアップ中にランダムに選択されネゴシエートされた UDP ポートで、該当するデバイスと通信する必要があります。

この脆弱性は UDP ベースのサービス内部にあるため、攻撃者は巧妙に細工された要求を作成する前にハンドシェイクを実行するように要求されません。このため、攻撃者は攻撃の送信元アドレスを詐称できます。

- CTMS - CSCth60993（ 登録ユーザのみ）として文書化され、CVE ID として CVE-2011-0389 が割り当てられています。

XML-RPC のサービス拒否

XML-RPC のサービス拒否の脆弱性は、Cisco TelePresence Multipoint Switch デバイスに存在します。リモートの認証されていない攻撃者が、該当するデバイスに悪意のあるリクエストを送信し、コール ジオメトリ処理のクラッシュを引き起こします。攻撃者は TCP ポート 9000 で、該当するデバイスと通信する必要があります。

攻撃者は、TCP 3 ウェイ ハンドシェイクを実行し、有効なセッションを確立しなければ、この脆

弱性を悪用することはできません。

- CTMS - CSCtj44534 （ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2011-0390 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

CSCtf42008 - Unauthenticated Java Servlet Access Calculate the environmental score of					
CVSS Base Score - **10.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtf01253 - Unauthenticated Java Servlet Access Calculate the environmental score of					
CVSS Base Score - **10.0**					
Access Vecto	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact

r					
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCth61065 - Unauthenticated Arbitrary File Upload **Calculate the environmental score of**					
CVSS Base Score - **10.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtd75766 - Cisco Discovery Protocol Remote Code Execution **Calculate the environmental score of**					
CVSS Base Score - **7.9**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Adjacent Network	Medium	None	Complete	Complete	Complete
CVSS Temporal Score - **6.5**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtf97164 - Unauthorized Servlet Access **Calculate the environmental score of**					
CVSS Base Score - **8.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Partial	Partial	Complete
CVSS Temporal Score - **6.6**					

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCtg35825 - Java RMI Denial of Service
Calculate the environmental score of

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCth60993 - Real-Time Transport Control Protocol Denial of Service
Calculate the environmental score of

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCtj44534 - XML-RPC Denial of Service
Calculate the environmental score of

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **7.4**

Exploitability	Remediation Level	Report Confidence
Functional	Unavailable	Confirmed

影響

Java Servlet による不正なアクセス（CSCtf42008、CSCtf01253）の脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者によって、該当するデバイスが完全に制御される可能性があります。

任意のファイルの不正なアップロード（CSCth61065）の脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者によって、該当するデバイスに任意のファイルが作成されたり上書きされる可能性があります。これによって、該当するデバイスが攻撃者に完全に制御される可能性があります。

Cisco Discovery Protocol によるコードのリモート実行（CSCtd75766）の脆弱性の不正利用に成功した場合、認証されていない近接した攻撃者によって、該当するシステムが完全に制御される可能性があります。

不正な Servlet によるアクセス（CSCtf97164）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が、攻撃者の権限レベルでは制限されている操作をシステムで実行できる可能性があります。

Java RMI のサービス拒否（CSCtg35825）の脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者によって、すべての Web ベースのサービスがアクセス不能にされる可能性があります。

RTCP のサービス拒否（CSCth60993）の脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者によって、該当するデバイスですべてのアクティブ コールが終了させられる可能性があります。

XML-RPC のサービス拒否（CSCtj44534）の脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者によって、すべての現在のコールが終了させられ、今後のコールにデバイスが使用できなくな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

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。

次の Cisco TelePresence システム ソフトウェアの表の各列には、不具合の内容、修正を含む最初のリリース、本アドバイザリで報告されているすべてのセキュリティ問題およびその他のセキュリティ以外の問題を解決するために推奨されるリリースが記載されています。シスコはテーブルの「Recommended Releases」列のリリース、またはそれ以降のリリースにアップグレードすることを推奨します。

Vulnerability	Bug ID	Component	First Fixed Version	Recommended Release
Unauthenticated Java Servlet Access	CSCtf01253	CTMS	1.7.0	1.7.1
	CSCtf42008	CTMS	1.7.0	1.7.1
Unauthenticated Arbitrary File Upload	CSCth61065	CTMS	1.7.0	1.7.1
Cisco Discovery Protocol Remote Code Execution	CSCtd75766	CTMS	1.7.0	1.7.1
Unauthorized Servlet Access	CSCtf97164	CTMS	1.7.0	1.7.1
Java RMI JBOSS Denial of Service	CSCtg35825	CTMS	1.7.0	1.7.1
Real-Time Transport Control Protocol Denial of Service	CSCth60993	CTMS	1.7.0	1.7.1
XML-RPC Denial of Service	CSCtj44534	CTMS	1.7.2 – Estimated Availability is End of March 2011	1.7.2 – Estimated Availability is End of March 2011

Cisco TelePresence ソリューションの全コンポーネントを 1.7.1 以降にアップグレードすることを推奨します。

回避策

確認されている脆弱性には、デバイスやシステムで対処できる回避策はありません。

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 Mitigation Bulletin』にて参照できます。

http://www.cisco.com/warp/public/707/cisco-amb-20110223-telepresence.shtml

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下さい。

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。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、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項、または Cisco.com ダウンロード サイトの http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

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。ほとんどのお客様は、シスコのワールドワイド Web サイト上の Software Center からアップグレードを入手することができます。 http://www.cisco.com

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。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、 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。

本セキュリティ アドバイザリで報告されているすべての脆弱性は、シスコ内部で発見されたものです。

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://www.cisco.com/warp/public/707/cisco-sa-20110223-telepresence-ctms.shtml

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-bulletins@lists.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 1.1	2011-March-9	Advisory updated to provide new information regarding CSCtj44534 (CVE-2011-0390) and to provide estimated availability for software that will resolve this issue.
Revision 1.0	2011-February-23	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。