Cisco IOS Software and Cisco IOS XE Software EnergyWise Crafted Packet Denial of Service Vulnerability

Advisory ID: cisco-sa-20140806-energywise

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140806-energywise

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 2014 August 6 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 IOS および Cisco IOS XE ソフトウェアの EnergyWise モジュールの脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを発生させる可能性があります。

この脆弱性は、該当デバイス宛ての巧妙に細工された EnergyWise パケットが適切に解析されないことに起因します。攻撃者は、該当デバイスによって処理される巧妙に細工された EnergyWise 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。この脆弱性を不正利用することにより、攻撃者は該当デバイスのリロードを引き起こすことができる場合があります。

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。

この脆弱性に対する回避策はありません。

このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140806-energywise

該当製品

脆弱性が認められる製品

該当するリリースの Cisco IOS および Cisco IOS XE ソフトウェアが稼働し、EnergyWise 機能の使用が設定されているシスコ デバイスが、この脆弱性の影響を受けます。

EnergyWise 機能は、Cisco IOS デバイスおよび Cisco IOS XE デバイスにおいて、デフォルトでは有効になっていません。

Cisco IOS デバイスに EnergyWise が設定されているかどうかを確認するには、 **show run | include energywise** コマンドを使用します。次の例は、EnergyWise 機能を有効にするために必要な最小限の設定が適用されている Cisco IOS デバイスにおける、 **show run | include energywise** コマンドの出力例です。

```
Router#show run | include energywise
energywise domain test_domain security shared-secret 0 test123
```

注：EnergyWise ドメインの設定は、Cisco IOS デバイスで EnergyWise 機能を有効にするのに必要な最小限の設定です。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインし **show version** コマンドを実行してシステム バナーを表示させます。「Internetwork Operating System Software」、「Cisco IOS Software」あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。その後ろにイメージ名が括弧の間に表示され、続いてバージョンと Cisco IOS ソフトウェア リリース名が表示されます。他のシスコ デバイスでは、 **show version** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.0(1)M1 が稼働し、インストールされているイメージ名が C3900-UNIVERSALK9-M であることを示しています。

```
Router>show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version
15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
<output truncated>
```

脆弱性が認められない製品

Cisco EnergyWise Suite（旧称 JouleX Energy Manager ソリューション）に含まれている製品およびサービスは、この脆弱性の影響を受けません。

データセンター向け Cisco EnergyWise Management、分散型オフィス向け Cisco EnergyWise Management、Cisco EnergyWise Discovery Service、Cisco EnergyWise Optimization Service は、この脆弱性の影響を受けません。

Cisco IOS XR は、この脆弱性の影響を受けません。

他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

詳細

Cisco EnergyWise は、企業の IT ネットワークのエネルギー使用量を測定および制御するための、Cisco IOS ソフトウェアベースのプロトコルとして開発されました。

Cisco EnergyWise ネットワークでは、シスコ ネットワーキング デバイス、Power over Ethernet（PoE）エンドポイントのほか、ソフトウェア開発キット（SDK）を使用して作成されたエージェントを実行するエンドポイントなどのドメインにおいて、受電装置の電力使用量を EnergyWise がモニタおよび管理します。

Cisco IOS および Cisco IOS XE ソフトウェアの EnergyWise モジュールの脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを発生させる可能性があります。

この脆弱性は、該当デバイス宛ての巧妙に細工された EnergyWise パケットが適切に解析されないことに起因します。攻撃者は、該当デバイスによって処理される巧妙に細工された EnergyWise 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。この脆弱性を不正利用することにより、攻撃者は該当デバイスのリロードを引き起こすことができる場合があります。

該当デバイス宛ての UDP パケットと TCP パケットはどちらも、この脆弱性の不正利用に使用される可能性があります。該当デバイスを通過するトラフィックは、この脆弱性の不正利用に使用されることはありません。

Cisco IOS ソフトウェアと Cisco IOS XE ソフトウェアは、EnergyWise との IP バージョン 4（IPv4）通信をサポートします。

この脆弱性は、EnergyWise ドメイン メンバーとして設定されているデバイス宛ての IPv4 パケットによってのみ引き起こされます。IPv6 パケットを使用してこの脆弱性を引き起こすことはできません。

攻撃者は、TCP または UDP ポート 43440 で送信された IPv4 パケットを使用して、この脆弱性を不正利用する可能性があります。

この不正利用によって、Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアがリロードされ、サービス拒否（DoS）状態になることがあります。

この脆弱性は、Cisco Bug ID CSCup52101（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID CVE-2014-3327 が割り当てられています。

プロトコルとポートの詳細

Cisco EnergyWise ドメイン メンバーは、以下の 3 つの個別の通信チャネルを介して、他の EnergyWise 対応デバイスと通信します。

- ネイバー探索用の Cisco Discovery Protocol メッセージまたは UDP メッセージ
- 管理アプリケーション用の TCP パケット
- EnergyWise 対応エンドポイントに送信される、制御メッセージ用の TCP パケット

Cisco Discovery Protocol メッセージまたは UDP メッセージ

Cisco EnergyWise ドメイン メンバーは、Cisco Discovery Protocol メッセージ（有効になっている場合）または EnergyWise UDP メッセージを使用して、ネイバーを自動的に検出します。デフォルトでは、EnergyWise ドメイン メンバーで有効になっているのは UDP ポート 43440 です。

この脆弱性の不正利用に使用される可能性があるのは、ネイバー探索用に UDP ポート 43440 で送信されたパケットのみです。

注： **energywise domain** *domain* **security shared-secret 0** *secret* **protocol udp port** *udp-port-number* コマンドを使用して、EnergyWise デバイスがリッスンするデフォルトの UDP ポート番号（43440）を変更することもできます。

管理アプリケーション用の TCP パケット

また、ドメイン メンバーは、Cisco EnergyWise の管理 API（MAPI）用に管理ポートを設定することもできます。MAPI を使用しているアプリケーションは、ドメイン メンバーに設定されている管理ポートに接続し、そのポートを管理ワークステーションとドメイン メンバー間の通信に使用できます。

管理ポートは、デフォルトでは有効になっていません。管理者は、 **energywise management security shared-secret 0** *shared-secret* コマンドを使用して、このオプションを設定できます。この設定により、デフォルトが TCP ポート 43440 になります。

管理ポートが設定されている場合、TCP ポート 43440 で送信される管理パケットが、この脆弱性の不正利用に使用される可能性があります。

注： **energywise management security shared-secret 0** *shared-secret* **port** *tcp-port-number* コマンドを使用して、管理通信用に EnergyWise デバイスがリッスンする TCP ポート番号を変更することもできます。デフォルトは、TCP ポート 43440 です。

制御メッセージ用の TCP パケット

PoE エンドポイントや、SDK を使用して作成されたエージェントを実行するエンドポイントにクエリや制御メッセージを送信するように、Cisco EnergyWise ドメイン メンバーを設定することもできます。

ドメイン メンバーおよびエンドポイントは、AC 電源、DC 電源、または電源モジュールから電力を受け取ることができます。PoE ドメイン メンバーおよびエンドポイントは、PoE スイッチまたは Cisco EtherSwitch サービス モジュールからも電力を受け取ることができます。

Cisco EnergyWise ドメイン メンバーは、コンフィギュレーション コマンド **energywise endpoint security** *shared-secret* を使用して、エンドポイントと通信するように設定することができます。

設定すると、EnergyWise エンドポイント通信で TCP ポート 43440 が使用されます。EnergyWise エンドポイント通信は、デフォルトでは有効になっていません。

EnergyWise エンドポイント通信が設定されている場合、エンドポイントから TCP ポート 43440 で送信されるパケットが、この脆弱性の不正利用に使用される可能性があります。

注：エンドポイント通信用に設定されている EnergyWise ドメイン メンバーは、管理用に使用されるのと同じ TCP ソケットでリッスンします。EnergyWise 管理機能が設定されていない場合は、エンドポイント通信に使用されるデフォルトの TCP ポートを変更することはできません。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ 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組織の手助けとなる標準ベースの評価法です。

シスコでは、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、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

CSCup52101 - Cisco IOS Software EnergyWise Crafted Packet Denial of Service Vulnerability 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	

影響

この脆弱性が不正利用されると、該当するデバイスのリロードが引き起こされ、サービス拒否（DoS）状態になることがあります。

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場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

Cisco IOS ソフトウェア

Cisco IOS ソフトウェア テーブル（下記）の各行は Cisco IOS ソフトウェア トレインを示します。あるトレインが脆弱性を含む場合、修正を含む最初のリリースは「First Fixed Release」列に示されます。可能な限り、最新のリリースにアップグレードすることを推奨します。

Cisco IOS ソフトウェア チェッカーを利用して、特定の Cisco IOS ソフトウェア リリースに対応したシスコのセキュリティ アドバイザリを検索することができます。このツールは次の Cisco Security Intelligence Operations（SIO）ポータルで利用できます。
http://tools.cisco.com/security/center/selectIOSVersion.x

Major Release	Availability of Repaired Releases
Affected 12.0-Based Releases	First Fixed Release
There are no affected 12.0 based releases	
Affected 12.2-Based Releases	First Fixed Release
12.2EX	Vulnerable; migrate to any release in 12.2SEG Releases up to and including 12.2(55)EX2 are not vulnerable.
12.2EY	Vulnerable; migrate to any release in 15.1EY Releases up to and including 12.2(55)EY are not vulnerable.
12.2EZ	Releases up to and including 12.2(55)EZ are not vulnerable.
12.2IRB	Not vulnerable
12.2IRC	Not vulnerable
12.2IRD	Not vulnerable
12.2IRE	Not vulnerable
12.2IRF	Not vulnerable
12.2IRG	Not vulnerable
12.2IRH	Not vulnerable
12.2IRI	Not vulnerable
12.2IXG	Not vulnerable
12.2IXH	Not vulnerable
12.2MC	Not vulnerable
12.2MRA	Not vulnerable
12.2MRB	Not vulnerable

12.2SB	Not vulnerable
12.2SCA	Not vulnerable
12.2SCB	Not vulnerable
12.2SCC	Not vulnerable
12.2SCD	Not vulnerable
12.2SCE	Not vulnerable
12.2SCF	Not vulnerable
12.2SCG	Not vulnerable
12.2SCH	Not vulnerable
12.2SCI	Not vulnerable
12.2SE	Releases up to and including 12.2(55)SE9 are not vulnerable.
12.2SEG	Not vulnerable
12.2SG	Not vulnerable
12.2SGA	Not vulnerable
12.2SM	Not vulnerable
12.2SQ	Not vulnerable
12.2SRA	Not vulnerable
12.2SRB	Not vulnerable
12.2SRC	Not vulnerable
12.2SRD	Not vulnerable
12.2SRE	Not vulnerable
12.2STE	Not vulnerable
12.2SV	Not vulnerable
12.2SVD	Not vulnerable
12.2SVE	Not vulnerable
12.2SW	Not vulnerable
12.2SXF	Not vulnerable Please see IOS Software Modularity Patch
12.2SXH	Not vulnerable Please see IOS Software Modularity Patch
12.2SXI	Not vulnerable
12.2SXJ	Not vulnerable
12.2SY	Not vulnerable
12.2WO	Not vulnerable
12.2XNA	Please see Cisco IOS-XE Software Availability
12.2XNB	Please see Cisco IOS-XE Software Availability
12.2XNC	Please see Cisco IOS-XE Software Availability
12.2XND	Please see Cisco IOS-XE Software Availability
12.2XNE	Please see Cisco IOS-XE Software Availability
12.2XNF	Please see Cisco IOS-XE Software Availability
12.2XO	Not vulnerable
12.2ZYA	Not vulnerable
Affected 12.3-Based Releases	**First Fixed Release**
There are no affected 12.3 based releases	
Affected 12.4-Based Releases	**First Fixed Release**
There are no affected 12.4 based releases	
Affected 15.0-Based Releases	**First Fixed Release**
15.0EA	Not vulnerable
15.0EB	Not vulnerable
15.0EC	Not vulnerable
15.0ED	Vulnerable; First fixed in Release 15.2E

15.0EH	Vulnerable; First fixed in Release 15.2E
15.0EJ	Vulnerable; First fixed in Release 15.2E
15.0EK	Releases prior to 15.0(2)EK1 are vulnerable; Releases 15.0(2)EK1 and later are not vulnerable.First fixed in Release 15.2E
15.0EX	Vulnerable; First fixed in Release 15.2E Releases up to and including 15.0(1)EX3 are not vulnerable.
15.0EY	Not vulnerable
15.0EZ	Releases up to and including 15.0(1)EZ1 are not vulnerable.
15.0M	Not vulnerable
15.0MR	Not vulnerable
15.0S	Not vulnerable
15.0SE	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0SG	Not vulnerable
15.0SQC	Not vulnerable
15.0SY	Not vulnerable
15.0XA	Not vulnerable
15.0XO	Not vulnerable
Affected 15.1-Based Releases	**First Fixed Release**
15.1EY	Not vulnerable
15.1GC	Not vulnerable
15.1M	Not vulnerable
15.1MR	Not vulnerable
15.1MRA	Not vulnerable
15.1S	Not vulnerable
15.1SG	Vulnerable; First fixed in Release 15.2E
15.1SNG	Not vulnerable
15.1SNH	Not vulnerable
15.1SNI	Not vulnerable
15.1SY	15.1(1)SY4; Available on 31-OCT-14
15.1T	Not vulnerable
15.1XO	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
Affected 15.2-Based Releases	**First Fixed Release**
15.2E	15.2(3)E; Available on 23-OCT-14
15.2EA	Not vulnerable
15.2EB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2EY	Not vulnerable
15.2GC	Not vulnerable
15.2JA	Not vulnerable
15.2JAC	Not vulnerable
15.2JAX	Not vulnerable
15.2JB	Not vulnerable
15.2JN	Not vulnerable
15.2M	Not vulnerable
15.2S	Releases prior to 15.2(4)S3 are vulnerable; Releases 15.2(4)S3 and later are not vulnerable.
15.2SA	Not vulnerable
15.2SNG	Not vulnerable
15.2SNH	Not vulnerable
15.2SNI	Not vulnerable

15.2T	Not vulnerable
Affected 15.3-Based Releases	**First Fixed Release**
There are no affected 15.3 based releases	
Affected 15.4-Based Releases	**First Fixed Release**
15.4CG	Not vulnerable
15.4M	Not vulnerable
15.4S	Releases prior to 15.4(3)S are vulnerable; Releases 15.4(3)S and later are not vulnerable.
15.4T	Not vulnerable

Cisco IOS XE ソフトウェア

Affected Release	First Fixed Release
2.x	Not vulnerable
3.1.xSG	Not vulnerable
3.2.xSG	Not vulnerable
3.2.xSE	Not vulnerable
3.2.xSQ	Not vulnerable
3.2.xXO	Vulnerable
3.3.xSG	Vulnerable
3.3.xSQ	Not vulnerable
3.4.xSG	Vulnerable
3.5.xE	3.5.3E
3.2.xS	Not vulnerable
3.3.xS	Not vulnerable
3.4.xS	Not vulnerable
3.5.xS	Not vulnerable
3.6.xS	Not vulnerable
3.7.xS	Not vulnerable
3.8.xS	Not vulnerable
3.9.xS	Not vulnerable
3.10.xS	Not vulnerable
3.11.xS	Not vulnerable
3.12.xS	Not vulnerable

Cisco IOS XE リリースと Cisco IOS リリースのマッピングについては、Cisco IOS XE 2 リリース ノート、Cisco IOS XE 3S リリース ノート、Cisco IOS XE 3SG リリース ノートを、それぞれ http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html#wp2310700、http://www.cisco.com/en/US/docs/ios/ios_xe/3/release/notes/asr1k_rn_3s_sys_req.html#wp2999052、http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_24726.html#wp2570252 で入手できます。

サービス契約をご利用のお客様は、このアドバイザリの「修正済みソフトウェアの入手」セクションの手順に従ってシスコのサポート会社にお問い合わせください。

回避策

この脆弱性に対す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 Intelligence』にて参照できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=34962

修正済みソフトウェアの入手

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。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の特有の問題をご確認ください。

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。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 ライセンスの条項に従うことに同意したことになります。

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、Cisco.com の Software Navigator 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/cisco/software/navigator.html

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、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、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に関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償ア

ップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、E 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、シスコ ワールドワイドお問い合わせ先（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 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、ERNW GmbH の Ayhan Koca 氏と Matthias Luft 氏によって発見され、シスコに報告されました。

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

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140806-energywise

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- 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
- fulldisclosure@seclists.org

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2014-August-06	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サポート、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の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリ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。