Cisco Security Advisory: Cisco IOS Internet Key Exchange Vulnerability

Advisory ID: cisco-sa-20120328-ike

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

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 March 28 16:00 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアのインターネット キー エクスチェンジ（IKE）機能には、サービス拒否（DoS）の脆弱性があります。

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。

このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

注：2012 年 3 月 28 日の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開には 9 件の Cisco Security Advisory が含まれています。各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決する Cisco IOS ソフトウェア リリース、および 2012 年 3 月にバンドル公開したすべての脆弱性を解決する Cisco IOS ソフトウェア リリースを記載しています。

個々の公開リンクは、次のリンクにある「Cisco Event Response: Semi-Annual Cisco IOS

Software Security Advisory Bundled Publication」内に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

該当製品

脆弱性が存在する製品

Cisco IOS ソフトウェアを実行しているシスコ デバイスは、IKE バージョン 1（IKEv1）を使用するように設定されている場合、脆弱性が存在します。

IKEv1 はいくつかの機能で使用しています。その中には、次のようなさまざまなバーチャル プライベート ネットワーク（VPN）が挙げられます。

- LAN-to-LAN VPN
- リモート アクセス VPN（SSL VPN は含まず）
- Dynamic Multipoint VPN（DMVPN）
- Group Domain of Interpretation（GDOI）

デバイスで IKE が設定されているかどうかは、次の 2 つの方法で確認できます。

- 実行中のデバイスで IKE ポートが開いているか確認する
- デバイスの設定に IKE 機能が含まれているか確認する

実行中のデバイスで IKE ポートが開いているか確認する

デバイスに IKE が設定されているかどうかを確認する推奨方法は、 **show ip sockets** または **show udp** EXEC コマンドを実行します。デバイスの UDP ポート 500、UDP ポート 4500、UDP ポート 848、UDP ポート 4848 が開いている場合、デバイスは IKE パケットを処理しています。

次の例では、IPv4 または IPv6 のいずれかを使用して、UDP ポート 500 および UDP ポート 4500 で IKE パケットを処理しているデバイスを示します。

```
router# show udp
Proto        Remote      Port      Local       Port  In Out
Stat TTY OutputIF
 17       --listen--          192.168.130.21    500   0   0
1001011   0
 17(v6)   --listen--          UNKNOWN           500   0   0
1020011   0
 17       --listen--          192.168.130.21   4500   0   0
1001011   0
 17(v6)   --listen--          UNKNOWN          4500   0   0
1020011   0
!---  router#
```

デバイスの設定に IKE 機能が含まれているか確認する

Cisco IOS のデバイス設定に脆弱性があるかどうかを確認するには、管理者は IKE を使用する機能が少なくとも 1 つ以上あるかを確かめる必要があります。これは、 **show run | include crypto map|tunnel protection ipsec|crypto gdoi** イネーブル モード コマンドを使用して確認できます。こ

のコマンドの出力に、 *crypto map*、 *tunnel protection ipsec*、または *crypto gdoi* のいずれかが含まれる場合、そのデバイスには IKE の設定が含まれます。次の例では、IKE が設定されたデバイスを示します。

```
router# show run | include crypto map|tunnel protection
ipsec|crypto gdoi
crypto map CM 100 ipsec-isakmp
 crypto map CM
router#
```

Cisco IOS ソフトウェア リリースを確認する

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_teamRouter> 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
```

Cisco IOS ソフトウェアのリリース命名規則の追加情報は以下のリンクにある「White Paper: Cisco IOS and NX-OS Software Reference Guide」で確認できます。
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

脆弱性が存在しない製品

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、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

IKE プロトコルは、インターネット プロトコル セキュリティ（IPsec）を構成するプロトコルのひとつであり、通信セッションの暗号化または認証に使用する属性のネゴシエーションをするために使用されます。これらの属性には暗号化アルゴリズム、モード、共有キーが含まれます。IKE の実行の結果、暗号化キーを導き出すために使用する共有セッション シークレットが生成されます。

Cisco IOS ソフトウェアは IPv4 および IPv6 通信向けの IKE をサポートします。IKE 通信は次の

任意の UDP ポートを使用することができます。

- UDP ポート 500
- UDP ポート 4500、NAT トラバーサル（NAT-T）
- UDP ポート 848、Group Domain of Interpretation（GDOI）
- UDP ポート 4848、GDOI NAT-T

Cisco IOS ソフトウェアの IKEv1 機能には、認証されていないリモートの攻撃者が該当デバイスの再起動を引き起こす可能性のある脆弱性があります。

攻撃者は、このリストにあるいずれかの UDP ポートで IPv4 または IPv6 のいずれかを使用することで、この脆弱性を不正利用することができます。攻撃者は該当デバイスからの最初の応答を受信するか、または応答にアクセスする必要があるため、パケットのスプーフィングによる脆弱性の不正利用は制限されます。

この脆弱性は、Cisco Bug ID CSCts38429 として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-0381 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組織の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、自身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 計算ツールを次のリンクで提供しています。

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

CSCts38429 - Cisco IOS Software IKE DoS vulnerability CSCts38429 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、該当するデバイスが再起動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

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である場合、修正を含む最初のリリースは「First Fixed Release」列に示されます。「First Fixed Release for All Advisories in the March 2012 Bundled Publication」列は、その Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開で公開済みであるすべての脆弱性を修正する最初のリリースを示します。シスコは利用可能な最新のリリースへのアップグレードを推奨します。

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）ポータルで入手できます。
http://tools.cisco.com/security/center/selectIOSVersion.x

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication
12.2	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2B	Vulnerable; First fixed in Release 15.0M Releases up to and including 12.2(2)B7 are not vulnerable.	Vulnerable; First fixed in Release 15.0M
12.2BC	Vulnerable; First fixed in Release 15.0M Releases up to and including 12.2(4)BC1b are not vulnerable.	Vulnerable; First fixed in Release 15.0M
12.2BW	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2BX	Vulnerable; First fixed in Release 12.2SRE Releases up to and including 12.2(2)BX1 are not vulnerable.	Vulnerable; First fixed in Release 12.2SB
12.2BY	Vulnerable; First fixed in Release 15.0M Releases up to and including 12.2(2)BY3 are not vulnerable.	Vulnerable; First fixed in Release 15.0M
12.2BZ	Vulnerable; First fixed in Release 15.0M Releases up to and including 12.2(4)BZ2 are	Vulnerable; First fixed in Release 15.0M

	not vulnerable.	
12.2CX	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2CY	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2CZ	Vulnerable; migrate to any release in 12.0S	Vulnerable; First fixed in Release 12.0S
12.2DA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2DD	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2DX	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2EU	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2EW	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2EWA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2EX	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2EY	Not vulnerable	12.2(52)EY4
12.2EZ	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FX	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FY	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FZ	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2IRA	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRB	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRC	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRD	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRE	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRF	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2IRG	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRH	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXE	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXF	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXG	Vulnerable; contact your support organization	Vulnerable; contact your support organization

	per the instructions in Obtaining Fixed Software section of this advisory.	per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXH	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2JA	Not vulnerable	Not vulnerable
12.2JK	Not vulnerable	Not vulnerable
12.2MB	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2MC	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2MRA	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2MRB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2S	Note: Releases prior to 12.2(25)S1 are vulnerable; Releases 12.2(25)S1 and later are not vulnerable.	Releases prior to 12.2(30)S are vulnerable; Releases 12.2(30)S and later are not vulnerable.First fixed in Release 12.0S
12.2SB	Only releases 12.2(33)SB1 through 12.2(33)SB4 are vulnerable.	12.2(33)SB12
12.2SBC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SCA	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.2SCB	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.2SCC	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.2SCD	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.2SCE	12.2(33)SCE6	12.2(33)SCE6
12.2SCF	12.2(33)SCF2	12.2(33)SCF2
12.2SE	Not vulnerable*	12.2(55)SE5 *
12.2SEA	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEB	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEC	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SED	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEE	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEF	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEG	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SG	Not vulnerable	12.2(53)SG7; Available on 07-MAY-12
12.2SGA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SL	Not vulnerable	Not vulnerable
12.2SM	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SO	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SQ	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SRA	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2SRB	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2SRC	Vulnerable; First fixed in Release 12.2SRD	Vulnerable; First fixed in Release 12.2SRE
12.2SRD	12.2(33)SRD8	Vulnerable; First fixed in Release 12.2SRE
12.2SRE	12.2(33)SRE6	12.2(33)SRE6
12.2STE	Not vulnerable	Vulnerable; contact your support organization

		per the instructions in Obtaining Fixed Software section of this advisory.
12.2SU	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2SV	Not vulnerable	Releases up to and including 12.2(18)SV2 are not vulnerable.
12.2SVA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVE	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SW	Releases up to and including 12.2(21)SW1 are not vulnerable. Releases 12.2(25)SW10 and later are not vulnerable.First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.2SX	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXE	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXF	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXH	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXI	12.2(33)SXI9	12.2(33)SXI9
12.2SXJ	12.2(33)SXJ2	12.2(33)SXJ2
12.2SY	12.2(50)SY2; Available on 11-JUN-12	12.2(50)SY2; Available on 11-JUN-12
12.2SZ	Not vulnerable	Vulnerable; First fixed in Release 12.0S
12.2T	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2TPC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2XA	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XB	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XC	Not vulnerable	Vulnerable; First fixed in Release 15.0M

12.2XD	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XE	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XF	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.2XG	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XH	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XI	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XJ	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XK	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XL	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XM	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XNA	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNB	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNC	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XND	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNE	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNF	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XO	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2XQ	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XR	Not vulnerable	Releases prior to 12.2(15)XR are vulnerable; Releases 12.2(15)XR and later are not vulnerable.First fixed in Release 15.0M
12.2XS	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XT	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XU	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XV	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2XW	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2YA	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2YC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YE	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YK	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YO	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YP	Not vulnerable	Vulnerable; First fixed in Release 15.0M Releases up to and including 12.2(8)YP are not vulnerable.

12.2YT	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YW	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YX	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YY	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2YZ	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZB	Releases up to and including 12.2(8)ZB are not vulnerable.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZE	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2ZH	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.2ZJ	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZP	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZU	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZX	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2ZY	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2ZYA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.3	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3B	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3BC	Vulnerable; First fixed in Release 12.2SCE	Vulnerable; First fixed in Release 12.2SCE
12.3BW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.3JA	Not vulnerable	Vulnerable; First fixed in Release 12.4JA

12.3JEA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JEB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JEC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JED	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JK	Releases up to and including 12.3(2)JK3 are not vulnerable. Releases 12.3(8)JK1 and later are not vulnerable.First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3JL	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3JX	Not vulnerable	Not vulnerable
12.3T	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3TPC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3VA	Not vulnerable	Not vulnerable
12.3XA	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3XB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3XC	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3XD	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3XE	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3XF	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3XG	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3XI	Vulnerable; First fixed in Release 12.2SRE	Vulnerable; First fixed in Release 12.2SRE
12.3XJ	Vulnerable; migrate to any release in 12.4XN	Vulnerable; First fixed in Release 15.0M
12.3XK	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3XL	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3XQ	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3XR	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3XU	Vulnerable; First fixed in Release 12.4T Releases up to and including 12.3(8)XU1 are not vulnerable.	Vulnerable; First fixed in Release 12.4T
12.3XW	Vulnerable; migrate to any release in 12.4XN	Vulnerable; First fixed in Release 15.0M
12.3XX	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.3XY	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.3XZ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.3YD	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YF	Vulnerable; migrate to any release in 12.4XN	Vulnerable; First fixed in Release 15.0M
12.3YG	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YI	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M

12.3YJ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.3YK	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YM	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.3YQ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YS	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YT	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YU	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.3YX	Vulnerable; migrate to any release in 12.4XN	Vulnerable; First fixed in Release 15.0M
12.3YZ	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.3ZA	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
Affected 12.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.4	Vulnerable; First fixed in Release 15.0M	Vulnerable; First fixed in Release 15.0M
12.4GC	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JA	Not vulnerable	12.4(23c)JA4 12.4(25e)JA
12.4JAX	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4JDA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JDE	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JHC	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JK	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JL	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4JX	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4JY	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4JZ	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4MD	12.4(22)MD3; Available on 30-MAR-12	12.4(22)MD3; Available on 30-MAR-12

12.4MDA	12.4(24)MDA11	12.4(24)MDA11
12.4MDB	12.4(24)MDB5a	12.4(24)MDB5a
12.4MDC	Not vulnerable	Not vulnerable
12.4MR	Releases up to and including 12.4(9)MR are not vulnerable.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4MRA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4MRB	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4SW	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4T	12.4(15)T17 12.4(24)T7	12.4(15)T17 12.4(24)T7
12.4XA	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XB	Releases prior to 12.4(2)XB12 are vulnerable; Releases 12.4(2)XB12 and later are not vulnerable.First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XC	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XD	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XE	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XF	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XG	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XJ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XK	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XL	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XM	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XN	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XP	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XQ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XR	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 12.4T
12.4XT	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XV	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4XW	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XY	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4XZ	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4YA	Vulnerable; First fixed in Release 12.4T	Vulnerable; First fixed in Release 15.0M
12.4YB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4YD	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.4YE	12.4(24)YE3d	12.4(24)YE3d
12.4YG	12.4(24)YG4	12.4(24)YG4

Affected 15.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication
15.0M	15.0(1)M8	15.0(1)M8
15.0MR	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0MRA	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0S	15.0(1)S5 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(1)S5 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SA	Not vulnerable	Not vulnerable
15.0SE	Not vulnerable	15.0(1)SE1
15.0SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(2)SG2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SY	15.0(1)SY1	15.0(1)SY1
15.0XA	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
15.0XO	Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.1EY	Not vulnerable	15.1(2)EY2
15.1GC	15.1(2)GC2	15.1(2)GC2
15.1M	15.1(4)M3	15.1(4)M4; Available on 30-MAR-12
15.1MR	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1S	15.1(3)S2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(3)S2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SNG	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Not vulnerable
15.1T	15.1(1)T5; Available on 18-MAY-12 15.1(2)T5; Available on 27-APR-12 15.1(3)T3	15.1(3)T3
15.1XB	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1T
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.2GC	15.2(1)GC2	15.2(1)GC2
15.2S	15.2(1)S1 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.2(1)S1 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability

15.2T	15.2(1)T2 15.2(2)T1 15.2(3)T; Available on 30-MAR-12	15.2(1)T2 15.2(2)T1 15.2(3)T; Available on 30-MAR-12

* Cisco Catalyst 3550 シリーズ スイッチは Internet Key Exchange（IKE; インターネット キー エクスチェンジ）機能をサポートしており、デバイスがレイヤ 3 イメージを実行しているとき Cisco bug ID CSCts38429 の脆弱性に該当します。ただし、この製品はソフトウェア メンテナンス終了となっています。レイヤ 2 イメージを実行している Cisco 3550 シリーズ SMI スイッチは IKE をサポートしておらず、この脆弱性に該当しません。12.2SE ベースのソフトウェアが稼働している他の シスコ デバイスにも、この脆弱性はありません。

Cisco IOS XE ソフトウェア

Cisco IOS XE Software Release	First Fixed Release	First Fixed Release for All Advisories in the March 2012 Cisco IOS Software Security Advisory Bundled Publication
2.1.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.2.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.3.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.4.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.5.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
2.6.x	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
3.1.xS	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
3.1.xSG	Not vulnerable	Vulnerable; migrate to 3.2.2SG or later.
3.2.xS	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.

3.2.xSG	3.2.2SG	3.2.2SG
3.3.xS	Vulnerable; migrate to 3.4.2S or later.	Vulnerable; migrate to 3.4.2S or later.
3.3.xSG	Not Vulnerable	Not Vulnerable
3.4.xS	3.4.2S	3.4.2S
3.5.xS	3.5.1S	3.5.1S
3.6.xS	Not vulnerable	Not vulnerable

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、『Cisco IOS XE 2 Release Notes』、『Cisco IOS XE 3S Release Notes』、『Cisco IOS XE 3SG Release Notes』を参照してください。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、2012 年 3 月の Cisco IOS Software Security Advisory バンドル公開に含まれている脆弱性の影響を受けません。

回避策

この脆弱性に対する回避策はありません。

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。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 または http://www.cisco.com/public/sw-center/sw-usingswc.shtml 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。

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、Cisco.com 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、適切な処置について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。影響製品およびリリース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または修正が最適であるか、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。

- +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 を通して無償アップグレードをお求めください。

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、シスコ ワールドワイドお問い合わせ先を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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。

この脆弱性はシスコ内部でのテストによって発見されました。

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

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-20120328-ike

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電子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
- full-disclosure@lists.grok.org.uk

このアドバイザリに関する今後の更新があれば、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。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-March-28	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、Cisco.com 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 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。