SSL パケット処理中における Cisco IOS の複数の脆弱性

Low

アドバイザリーID : cisco-sa-20070522-SSL

初公開日 : 2007-05-22 13:00

バージョン 1.4 : Final

CVSSスコア : 3.3

回避策 : No Workarounds available

Cisco バグ ID : CSCsb12598 CSCsb40304 CSCsd92405

CVE-2007-2813

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 IOS デバイスは、不正形式の Secure Sockets Layer（SSL）パケットを処理するとクラッシュする可能性があります。 悪意のあるクライアントがこれらの脆弱性を悪用するためには、脆弱性のあるデバイスとの SSL プロトコル交換中に不正形式のパケットを送信する必要があります。

これらの脆弱性の何れかの正常な繰り返された利用は支えられたサービス拒否（DoS）の原因となるかもしれません; ただしデータまたはデバイスの機密保持か統合を妥協すると、脆弱性は知られていません。 これらの脆弱性を悪用しても、暗号化済みの情報を攻撃者が復号化することはできないと考えられます。

Cisco IOS に該当する脆弱性は次のものです。

- ClientHello メッセージの処理：この問題は、Cisco Bug ID CSCsb12598（登録ユーザ専用）に記載されています。
- ChangeCipherSpec メッセージの処理：この問題は、Cisco Bug ID CSCsb40304（登録ユーザ専用）に記載されています。
- Finished メッセージの処理：この問題は、Cisco Bug ID CSCsd92405（登録ユーザ専用）に記載されています。

Cisco では、該当するお客様用に、これらの脆弱性に対応する無償ソフトウェアを提供しております。 これらの脆弱性に対しては、影響を緩和するための回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL で掲示されます

注: このアドバイザとともに、関連するアドバイザリが公開されています。 この追加のアドバイザリは、Cisco IOS に影響を与える暗号化関連の脆弱性についても説明しています。 この関連アドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto

該当製品

脆弱性のある製品

これらの脆弱性は、Cisco IOS ソフトウェアが稼働していて、SSL プロトコルを使用するように設定されているすべての Cisco 製デバイスに該当します。 Cisco IOS のアプリケーション層プロトコルのうち、SSL を使用するものは次のとおりです。

- Hyper Text Transfer Protocol over SSL（HTTPS）。 これは、SSL を採用した最も一般的に使用されるプロトコルです。
- SSL サポート付き Cisco Network Security（CNS）エージェント
- HTTPS 認証プロキシのファイアウォール サポート
- Cisco IOS クライントレス SSL VPN（WebVPN）サポート

セキュリティ実装に暗号化を使用していても SSL を使用していないその他のプロトコルは、これらの脆弱性には該当しません。 特に、IPSec と Secure Shell（SSH; セキュア シェル）は該当しません。

Cisco IOS 製品で実行されているソフトウェアを確認するには、デバイスにログインし、show version コマンドを発行してシステム バナーを表示します。 Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。 出力の次の行には、カッコに囲まれたイメージ名が表示され、その後にバージョンと Cisco IOS リリース名が続きます。 その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

この脆弱性に該当するのは、暗号化機能セットを含む Cisco IOS イメージのみです。 暗号化サポートを含む IOS イメージを実行している場合は、この脆弱性に該当しません。

Cisco IOS 機能セットの命名規則では、暗号化サポートを含む IOS イメージの機能識別子フィールドに「K8」または「K9」の文字が入ります。

次の例は、暗号化サポートを含む IOS イメージを実行しているデバイスからの出力例です。

```
Router>show version
Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(14)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 31-Mar-05 08:04 by yiyan
```

機能セット識別子（IK9S）に「K9」が含まれているので、この機能セットには暗号化サポートが含まれていることがわかります。

Cisco IOS ソフトウェア リリースの命名方法に関する詳細については、次のリンクを参照してください。 http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml。

該当するいずれかのサービスがデバイス上で有効になっているかどうかを認識する方法は次のとおりです。

Hyper Text Transfer Protocol over SSL（HTTPS）

デバイスに有効に なる HTTPS があったかどうか確認するためにコマンド `show run` 入力して下さい `| IP HTTP` 。 次の例は、HTTPS が有効になっているデバイスからの出力結果を示しています。

```
Router#show run | include secure-server
ip http secure-server
```

次の例は、HTTPS が有効になっていないデバイスからの出力結果を示しています。

```
Router#show run | include secure-server
no ip http secure-server
```

SSL サポート付き CNS エージェント

SSL サポート付き CNS エージェントは、暗号化をサポートする Cisco IOS イメージが稼働しているデバイスでのみ有効にできます。 次の例は、SSL をサポートするように CNS エージェントが設定されているデバイスからの出力結果を示しています。

```
Router#show run | include cns config initial
cns config initial 10.1.1.1 encrypt no-persist
```

出力に encrypt キーワードが含まれていない場合は、CNS エージェントに脆弱性はありません。

HTTPS 認証プロキシのファイアウォール サポート

デバイスで HTTPS の認証プロキシが有効になっているかどうかを判別するには、show ip auth-proxy configuration コマンドを入力します。 次の例は、HTTPS の認証プロキシが有効になっているデバイスからの出力結果を示しています。

```
Router#show ip auth-proxy configuration
Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name my_pxy
http list not specified auth-cache-time 1 minutes
```

このコマンドを実行しても出力が生成されない場合、HTTPS の認証プロキシは有効になっていません。

Cisco IOS クライントレス SSL VPN（WebVPN）拡張サポート

デバイスで Cisco IOS クライントレス SSL VPN（WebVPN）拡張サポートが有効になっているかどうかを判別するには、show webvpn gateway コマンドを入力します。 次の例は、Cisco IOS クライントレス SSL VPN（WebVPN）拡張サポートが有効になっているデバイスからの出力結果を示しています。

```
Router#show webvpn gateway

Gateway Name                    Admin  Operation
------------                    -----  ---------
web-server                      up     up
```

このコマンドを実行しても出力が生成されない場合、Cisco IOS クライントレス SSL VPN（WebVPN）拡張サポートは有効になっていません。

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

SSL とは、2 つのホスト間での接続の安全性を高める設計になっているプロトコルです。 SSL プロトコルは、RFC4346 で定義されています。 このアドバイザリを理解するためには必要ではありませんが、RFC4346 のセクション「7.3 handshake Protocol Overview」および同セクション内の図 1 を確認することを推奨いたします。 RFC4346 のテキストは、次のリンク先で確認できます。 http://tools.ietf.org/html/rfc4346#section-7.3。

攻撃者は TCP 接続の確立後、ユーザ名/パスワードまたは証明書などの認証クレデンシャルの交換前にこれらの脆弱性の悪用を開始できます。 完全な TCP スリーウェイ ハンドシェイクの要求事項を満たすことにより、スプーフィング IP アドレスによってこれらの脆弱性が悪用される可能性を低減できます。

SSL セッションがすでに確立していれば、攻撃対象である 2 つのデバイス間のトラフィックを攻

撃者が傍受しても、これらの脆弱性を悪用できません。SSL はこのような注入からデバイスを保護します。 ただし、このような攻撃によって、既存セッションが TCP RST などを介して異常終了する場合があります。 この場合、攻撃者は新しい SSL セッションが確立されるまで待機し、新しい SSL セッションの開始時に悪意のあるパケットを注入することにより、脆弱性の悪用を試みる可能性があります。

ClientHello メッセージの処理によってクラッシュする場合がある

脆弱性のあるデバイスは、不正形式の ClientHello メッセージを処理するとクラッシュする可能性があります。 ClientHello メッセージはまず、クライアントがサーバに接続すると送信されます。それはまた SSL セッションが設定された後送信 することができます; そのような場合、メッセージは暗号化されたトンネルの内で送信 されます。

この脆弱性は、Cisco Bug ID CSCsb12598（登録ユーザ専用）に記載されています。

ChangeCipherSpec メッセージの処理によってクラッシュする場合がある

脆弱性のあるデバイスは、不正形式の ChangeCipherSpec メッセージを処理するとクラッシュする可能性があります。 ChangeCipherSpec メッセージは、ClientHello メッセージおよび ServerHello メッセージの交換後にのみ送信できます。 ほとんどの場合、ChangeCipherSpec メッセージは暗号化されたトンネル内で送信されます。

この脆弱性は、Cisco Bug ID CSCsb40304（登録ユーザ専用）に記載されています。

Finished メッセージの処理によってクラッシュする場合がある

脆弱性のあるデバイスは、不正形式の Finished メッセージを処理するとクラッシュする可能性があります。 このメッセージは、SSL ハンドシェイクの一部としてのみ送信できますが、最初のメッセージとして送信することはできません。 Finished メッセージは常に、暗号化されたトンネル内で送信されます。

この脆弱性は、Cisco Bug ID CSCsd92405（登録ユーザ専用）に記載されています。

脆弱性スコア評価の詳細

Cisco では、Common Vulnerability Scoring System（CVSS）に基づき、このアドバイザリで説明されている脆弱性のスコアを評価しました。

Cisco では基本スコアと現状スコアを評価します。 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。

Cisco PSIRT は、すべてのケースにおける重みを「標準」に設定します。 特定の脆弱性の環境的

影響を判断する際には、重みパラメータを適用することを推奨します。

CVSS は、脆弱性の重大度を伝える標準ベースのスコア評価方式であり、対応の緊急度や優先度を判断するのに役立ちます。

Cisco は http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html で CVSS に関する追加質問に答えるために FAQ を提供しました。

Cisco はまた http://tools.cisco.com/security/center/cvssCalculator.x で個々 の ネットワークのための環境影響の計算を助けるように CVSS カルキュレータを提供しました。

CSCsb12598：Processing ClientHello messages CSCsb12598 の環境スコアを計算する						
CVSS 基本スコア：3.3						
攻撃元区分	攻撃条件の複雑さ	認証	機密性への影響	完全性への影響	可用性への影響	影響の重み
Remote	低	不要	なし	なし	Complete	Normal
現状スコア：2.7						
攻撃される可能性		利用可能な対策のレベル		Report Confidence		
機能する		正式		確認済		

CSCsb40304：Processing ChangeCipherSpec messages CSCsb40304 の環境スコアを計算する						
CVSS 基本スコア：3.3						
攻撃元区分	攻撃条件の複雑さ	認証	機密性への影響	完全性への影響	可用性への影響	影響の重み
Remote	低	不要	なし	なし	Complete	Normal
現状スコア：2.7						
攻撃される可能性		利用可能な対策のレベル		Report Confidence		
機能する		正式		確認済		

CSCsd92405：Processing Finished messages CSCsd92405 の環境スコアを計算する						
CVSS 基本スコア：3.3						
攻撃元区分	攻撃条件の複雑さ	認証	機密性への影響	完全性への影響	可用性への影響	影響の重み
Remote	低	不要	なし	なし	Complete	Normal

現状スコア：2.7		
攻撃される可能性	利用可能な対策のレベル	Report Confidence
機能する	正式	確認済

回避策

ここで説明されている脆弱性の影響を受けないようにデバイスを保護する唯一の方法は、該当するサービスを無効にすることです。 ただし、デバイスの通常のメンテナンスと運用がこれらのサービスに依存している場合、回避策はありません。

該当するデバイスへの不正なホストからのアクセスを防ぐことにより、これらの脆弱性の影響を緩和できます。 ネットワーク内の Cisco デバイスに導入できる追加の緩和策については、このアドバイザリに関連する、次の Cisco 適用対応策速報を参照してください。 この関連ドキュメントは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070522-SSL

コントロール プレーン ポリシング（CoPP）

コントロール プレーン ポリシング： **コントロール プレーン ポリシング（CoPP）**をサポートする IOS ソフトウェア バージョンでは、管理と制御のプレーンに対する攻撃からデバイスを保護するように設定できます。 CoPP は、Cisco IOS リリース トレイン 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T で使用できます。

次の CoPP の例では、permit アクションがあり悪用パケットと一致する ACL エントリがポリシー マップの drop 機能によって廃棄されますが、「deny」アクション（表示なし）に一致するパケットはポリシー マップ drop 機能には該当しません。

```
Router#show webvpn gateway

Gateway Name                        Admin  Operation
------------                        -----  ---------
web-server                          up     up
```

Cisco IOS トレイン 12.0S、12.2S、および 12.2SX では、ポリシー マップの構文は次のように異なります。

```
Router#show webvpn gateway

Gateway Name                        Admin  Operation
------------                        -----  ---------
web-server                          up     up
```

注： 上の CoPP の例では、「permit」アクションがあり悪用パケットと一致する ACL エントリがある場合、ポリシー マップの drop 機能によってこれらのパケットは廃棄されますが、「deny」アクションと一致するパケットはポリシー マップ drop 機能には該当しません。

CoPP 機能の設定と使用方法についての詳細は、次のリンク先で確認できます。 http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html および http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html。

Access Control List (ACL; アクセス コントロール リスト)

アクセス コントロール リスト (ACL) を使用して、これらの脆弱性に対する攻撃を緩和できます。 ACL では、正規の送信元からのパケットのみがデバイスに到達でき、他のすべてのパケットは廃棄されるように指定できます。 次の例は、信頼できる送信元からの正規の SSL セッションを許可し、他のすべての SSL セッションを拒否する方法を示しています。

```
Router#show webvpn gateway

Gateway Name                        Admin   Operation
------------                        -----   ---------
web-server                          up      up
```

修正済みソフトウェア

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 およびそれ以降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せください。

Cisco IOS ソフトウェアの表 (下掲) の各行には、リリース トレインが記載されています。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース (「第 1 修正済みリリース」) とそれぞれの提供日が「リビルド」列と「メンテナンス」列に記載されます。 特定の列に記されているリリースよりも古い (第 1 修正済みリリースより古い) トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 このようなリリースは、少なくとも、示されているリリース以上 (最初の修正リリース ラベル以上) にアップグレードしてする必要があります。

「リビルド」および「メンテナンス」という用語の詳細は、次の URL を参照してください。

http://www.cisco.com/warp/public/620/1.html

メジャー リリース	修正済みリリースの入手可能性	
該当する 12.0 ベースのリリース	リビルド	メンテナンス
12.0T	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.0WC	12.0(5)WC17	
12.0XE	脆弱性あり; 12.1(26)E8 またはそれ以降への移行する	
12.0XH	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.0XI	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.0XK	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.0XL	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.0XN	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.0XQ	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.0XR	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.0XV	脆弱性あり; 12.2(46) またはそれ以降への移行する	
該当する 12.1 ベースのリリース	リビルド	メンテナンス
12.1	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.1AY	脆弱性あり; 12.1(22)EA9 またはそれ以降への移行する	
12.1CX	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.1E	12.1(26)E8	
	12.1(27b)E2; 利用可能 な 25-June-07	
12.1EA	12.1(22)EA9	
12.1EB	12.1(26)EB2; 利用可	

	能 な 30-July-07	
12.1EC	脆弱性あり; 12.3(21)BC またはそれ以降への移行する	
12.1EW	脆弱性あり; 12.2(25)EWA9 またはそれ以降への移行する	
12.1EX	脆弱性あり; 12.1(26)E8 またはそれ以降への移行する	
12.1EY	脆弱性あり; 12.1(26)E8 またはそれ以降への移行する	
12.1T	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.1XC	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.1XD	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.1XF	脆弱性あり; 移行する 12.3(22) またはそれ以降	
12.1XG	脆弱性あり; 移行する 12.3(22) またはそれ以降	
12.1XH	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.1XI	脆弱性あり; 12.2(46) またはそれ以降への移行する	
12.1XJ	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.1XL	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.1XM	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.1XP	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.1XQ	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.1XT	脆弱性あり; 移行する to12.3(22) またはそれ以降	
12.1XU	脆弱性あり; 移行する to12.3(22) またはそれ以降	
12.1YB	脆弱性あり; 移行する to12.3(22) またはそれ以降	
12.1YC	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.1YD	脆弱性あり; 移行する to12.3(22) またはそれ以降	
12.1YE	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.1YF	脆弱性あり; 12.3(22) またはそれ以降への移行する	

12.1YI	脆弱性あり; 移行する to12.3(22) またはそれ以降	
該当する 12.2 ベースのリリース	**リビルド**	**メンテナンス**
12.2	12.2(40a)	12.2(46)
12.2B	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2BC	脆弱性あり; 12.3(21)BC またはそれ以降への移行する	
12.2BW	脆弱性あり; 移行する 12.3(22) またはそれ以降	
12.2BY	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2BZ	脆弱性あり; contact TAC	
12.2CX	脆弱性あり; 12.3(21)BC またはそれ以降への移行する	
12.2CY	脆弱性あり; 12.3(21)BC またはそれ以降への移行する	
12.2CZ	脆弱性あり; contact TAC	
12.2DD	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2EW	脆弱性あり; 12.2(25)EWA9 またはそれ以降への移行する	
12.2EWA	12.2(25)EWA9	
12.2EX	脆弱性あり; 12.2(25)SEE3 またはそれ以降への移行する	
12.2EY	脆弱性あり; 12.2(25)SEE3 またはそれ以降への移行する	
12.2EZ	脆弱性あり; 12.2(25)SEE3 またはそれ以降への移行する	
12.2FX	脆弱性あり; 12.2(25)SEE3 またはそれ以降への移行する	
12.2FY	脆弱性あり; 12.2(25)SEG2 またはそれ以降への移行する	
12.2FZ	脆弱性あり; 12.2(35)SE またはそれ以降への移行する	
12.2JA	脆弱性あり; 12.3(11)JA またはそれ以降への移行する	
12.2JK	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.2S	12.2(14)S13a	12.2(25)S12
	12.2(18)S0a	
	12.2(20)S9a	

12.2SB	12.2(28)SB4b	
	12.2(31)SB2	
12.2SBC	脆弱性あり; 12.2(31)SB2 またはそれ以降への移行する	
12.2SE		12.2(35)SE
12.2SEA	脆弱性あり; 12.2(25)SEE3 またはそれ以降への移行する	
12.2SEB	脆弱性あり; 12.2(25)SEE3 またはそれ以降への移行する	
12.2SEC	脆弱性あり; 12.2(25)SEE3 またはそれ以降への移行する	
12.2SED	脆弱性あり; 12.2(25)SEE3 またはそれ以降への移行する	
12.2SEE	12.2(25)SEE3	
12.2SEF	脆弱性あり; 12.2(35)SE またはそれ以降への移行する	
12.2SEG	12.2(25)SEG2	
12.2SG	12.2(37)SG	
12.2SGA	12.2(31)SGA2; 利用可能 な 11-June-2007	
12.2SRA	12.2(33)SRA2	
12.2SU	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2SV	12.2(28)SV2	
	12.2(29)SV3	
12.2SW	12.2(25)SW9	
12.2SX	脆弱性あり; 12.2(18)SXE6a またはそれ以降への移行する	
12.2SXA	脆弱性あり; 12.2(18)SXE6a またはそれ以降への移行する	
12.2SXB	脆弱性あり; 12.2(18)SXE6a またはそれ以降への移行する	
12.2SXD	脆弱性あり; 12.2(18)SXE6a への移行する	
12.2SXE	12.2(18)SXE6a	
12.2SXF	12.2(18)SXF8	
12.2SY	脆弱性あり; 12.2(18)SXE6a またはそれ以降への移行する	
12.2T	脆弱性あり; 移行する 12.3(22) またはそれ以降	
12.2TPC	12.2(8)TPC10b	
12.2XA	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.2XB	脆弱性あり; 12.3(22) またはそれ以降への	

	移行する
12.2XD	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XE	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XF	脆弱性あり; 12.3(21)BC またはそれ以降への移行する
12.2XG	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XH	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XI	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XJ	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2 XK	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XL	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XM	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XN	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XQ	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XR	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XS	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XT	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XU	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XV	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2XW	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2YA	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2YB	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2YC	脆弱性あり; 12.3(22) またはそれ以降への移行する
12.2YD	脆弱性あり; 12.4(10) またはそれ以降への移行する
12.2YE	脆弱性あり; 12.2(25)S12 またはそれ以降への移行する

12.2YF	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.2YJ	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.2YL	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YM	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YN	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YQ	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YR	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YU	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YV	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YW	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YX	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YY	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2YZ	脆弱性あり; contact TAC	
12.2ZA	脆弱性あり; 12.2(18)SXE6a またはそれ以降への移行する	
12.2ZB	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2ZD	脆弱性あり; contact TAC	
12.2ZE	脆弱性あり; 12.3(22) またはそれ以降への移行する	
12.2ZF	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2ZH	脆弱性あり; contact TAC	
12.2ZJ	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2ZL	脆弱性あり; contact TAC	
12.2ZN	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.2ZU	脆弱性あり; contact TAC	
12.2ZV	脆弱性あり; contact TAC	
12.2ZW	脆弱性あり; contact TAC	
12.2ZX	脆弱性あり; contact TAC	
該当する 12.3	**リビルド**	**メンテナンス**

ベースのリリース		
12.3	12.3(21a)	12.3(22)
12.3B	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.3BC	12.3(17b)BC5	12.3(21)BC
12.3JA		12.3(11)JA
12.3JEA		12.3(8)JEA
12.3JK	脆弱性あり; contact TAC	
12.3JX	脆弱性あり; contact TAC	
12.3T	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.3TPC	12.2(8)TPC10b	
12.3XA	脆弱性あり; contact TAC	
12.3XB	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.3XC	脆弱性あり; contact TAC	
12.3XD	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.3XE	脆弱性あり; contact TAC	
12.3XF	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.3XG	脆弱性あり; contact TAC	
12.3XH	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.3XI	脆弱性あり; contact TAC	
12.3XJ	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3XK	脆弱性あり; contact TAC	
12.3XQ	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.3XR	脆弱性あり; contact TAC	
12.3XS	脆弱性あり; 12.4(10) またはそれ以降への移行する	
12.3XU	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3XW	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3XX	12.3(8)XX2d	
12.3YA	脆弱性あり; contact TAC	
12.3YD	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YF	脆弱性あり; 12.4(11)T またはそれ以降への移行する	

12.3YG	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YH	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YI	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YK	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YQ	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YS	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YT	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YU	脆弱性あり; contact TAC	
12.3YX	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.3YZ	脆弱性あり; contact TAC	
該当する 12.4 ベースのリリース	**リビルド**	**メンテナンス**
12.4	12.4(3h)	12.4(10)
	12.4(7d)	
	12.4(8c)	
12.4T	12.4(4)T6	12.4(11)T
	12.4(6)T7	
	12.4(9)T3	
12.4XA	脆弱性あり; 12.4(11)T またはそれ以降への移行する	
12.4XB	脆弱性あり; contact TAC	
12.4XC	12.4(4)XC4	
12.4XD	12.4(4)XD5	
12.4XE	脆弱性あり; contact TAC	

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

これらの脆弱性は、Cisco の社内テストで発見されたものです。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL

改訂履歴

リビジョン 1.4	2008-June-27	リンクおよび冗漫を取除く更新済要約。
リビジョン 1.3	2007 年 10 月 19 日	12.4 のリビルド リリースを 12.4(3)g から 12.4(3h) に置き換え。
リビジョン 1.2	2007 年 6 月 27 日	12.2SXF の第 1 修正済みリリースを、12.2(18)SXF7 から 12.2(18)SXF8 に変更。
リビジョン 1.1	2007 年 5 月 25 日	修正 IOS リリースを更新。
リビジョン 1.0	2007 年 5 月 22 日	初回公開リリース

利用規約