Cisco IOSソフトウェア 巧妙に細工された 暗号化 パケット サービス拒否の脆弱性

High	**アドバイザリーID :** cisco-sa-20090923-tls **初公開日 :** 2009-09-23 16:00 **バージョン 1.1 :** Final **CVSSスコア :** 7.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCsq24002	CVE-2009-2871

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 IOSÂ® ソフトウェアは攻撃者が Cisco IOSデバイスがリモートで 巧妙に細工された 暗号化パケットを送信 することによってリロードしますことを可能にする可能性がある脆弱性が含まれています。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls で掲示されます。

注: 2009 年 9 月 23 日の IOS アドバイザリ バンドル公開には 11 件の Security Advisory が含まれています。 10 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、 1 件は Cisco Unified Communications Manager の脆弱性に対処するものです。 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リリースを記載しています。

"Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" の個々の公開リンクは次のリンク内に掲載されています:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

該当製品

脆弱性のある製品

Cisco IOSソフトウェアの実行するデバイスによって影響を受けるバージョンは次の機能の何

れかと敏感もし設定するならです:

- セキュア ソケット レイヤ（SSL）バーチャル プライベート ネットワーク（VPN）
- セキュア シェル（SSH）
- インターネット キー エクスチェンジ（IKE）暗号化された一時的な情報

注: WebVPN および SSL VPN より他の SSL/HTTPS 関連機能はこの脆弱性から影響を受けません。

SSLVPN がデバイスで、デバイスへのログイン判別し有効に なる、Command Line Interface（CLI）コマンド **show running-config を**発行するためかどうか **| webvpn を含んで下さい**。 デバイスが出力それから SSLVPN を設定されればおよび戻せばデバイスは脆弱かもしれません。 脆弱 な コンフィギュレーションはデバイスが Cisco IOS WebVPN（リリース 12.3(14)T で導入される）または Cisco IOS SSL VPN をサポートしているかどうかによって変わります（リリース 12.4(6)T で導入される）。 次のメソッドはデバイスが脆弱であるかどうか確認する方法を記述します:

「**show running-config** からの出力 **| webvpn を**」含まれています「**webvpn イネーブルが含んで下さい**」それからデバイスがオリジナル Cisco IOS WebVPN で設定される。 デバイスが脆弱であるかどうか判別する唯一の方法は webvpn がコマンド「**webvpn イネーブル**」によって有効に なること、そして「**ssl トラストポイント**」が設定されたことを確認するために「show running-config」の出力を検査することです。 次の例は Cisco IOS WebVPN で設定される脆弱な デバイスを示したものです:

```
webvpn enable
!
webvpn
 ssl trustpoint TP-self-signed-29742012
```

「show running-config からの出力 | webvpn を」含まれています「webvpn ゲートウェイ <word> が含んで下さい」それからデバイスが Cisco IOS SSL VPN 機能をサポートしている。 デバイスは「webvpn ゲートウェイ」セクションがの少なくとも 1 つで「インサービス」コマンドある場合脆弱です。 次の例は Cisco IOS SSL VPN で設定される脆弱 な デバイスを示したものです:

```
Router# show running | section webvpn
webvpn gateway Gateway
 ip address 10.1.1.1 port 443
 ssl trustpoint Gateway-TP
 inservice
 !
Router#
```

Cisco IOS SSL VPN をサポートするデバイスは「**インサービス**」webvpn gateway コマンドが含まれていることを設定される「**webvpn ゲートウェイ**」かすべての設定された「webvpn ゲートウェイ」がない場合脆弱ではないです。

、SSH が有効に された 使用 **show ip ssh コマンド**だったかどうか次の例に示すように確認す

るため:

```
Router#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
```

IKE 暗号化された一時的な情報 機能が有効に なったかどうか確認するために、**show running-config を**使用して下さい **|** 次の通り **rsa-encr コマンドを含んで下さい**:

```
Router#show running-config | inc rsa-encr
 authentication rsa-encr
```

Cisco 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、機器にログインし 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 "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Cisco 機器では、 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。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

!--- output truncated
```

次の例は C1841-ADVENTERPRISEK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.4(20)T を実行している Cisco製品を指定したものです:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます: http://www.cisco.com/warp/public/620/1.html。

脆弱性を含んでいないことが確認された製品

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から影響を受けません。

Cisco IOS XR ソフトウェアはこの脆弱性から影響を受けません。

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

SSLVPN か SSH のために設定される Cisco IOSデバイスは TCPポート 443（SSLVPN）または TCPポート 22（SSH）の特別に 巧妙に細工された TCPパケットを受け取るときリロードするかもしれません。 脆弱性が正常に不正利用されることができるようにこれらの機能の関連する TCPポート番号への 3方向ハンドシェイクの完了が必要となります; ただし、認証が必要となりません。 IKE 暗号化された一時的な情報のために設定される Cisco IOSデバイスはポート 500 または 4500 の特別に 巧妙に細工された UDP パケットを受信するときリロードするかもしれません（もし設定するなら NAT 走査（NAT-T）のために）。

この脆弱性 Cisco バグ ID CSCsq24002（登録ユーザのみ）で文書化されています、よくある脆弱性および公開（CVE）識別子 CVE-2009-2871 は割り当てられました。

回避策

利用可能 な 回避策は影響を受けた機能をディセーブルにし、VTY アクセスコントロール アクセス・コントロール・リストの使用の SSH アクセスを保護すること以外ありません。

SSL VPN 使用をディセーブルにする **webvpn enable コマンドを**使用しないで下さい。

Cisco IOS の場合 SSH サーバはコマンド **crypto key zeroize rsa の**適用によって間、コンフィギュレーションモードでディセーブルにすることができます。 SSH サーバは RSA キーペアを作成した上で自動的に有効に なります。 RSA キーをゼロにすることは完全に SSH サーバをディセーブルにする唯一の方法です。

SSH サーバ on Cisco IOS software へのアクセスはまた有効な転送 プロトコルとして SSH を取除くことによってディセーブルにすることができます。 このアクションは VTY ラインの許可された転送のリストから取除かれる「ssh」との transport input コマンドの再適用によって間、コンフィギュレーションモードですることができます。 次に、例を示します。

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

SSH サーバの機能性が望まれる場合、サーバへのアクセスは特定の出典 IP アドレスに制限 されるか、または VTY 行のアクセス コントロール リスト（ACL）の使用によって次の URL に示すように完全にブロックすることができます:
http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html#xtocid14

ACL の設定に関する詳細は Cisco の公共 Webサイトで見つけることができます:

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

以下は VTY access-list の例です:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

前例では、10.1.1.0/24 ネットワークだけ Cisco IOSデバイスへの SSH に許可されます。

IKE 暗号化された一時的な情報をディセーブルにするために次の例に示すように ISAKMPポリシーの下で**認証 rsa-encr コマンドを**、使用しないで下さい:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

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、Cisco IOS のリリース 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（および、

それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 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。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャーリリース	修正済みリリースの入手可能性	
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）	**推奨リリース**
該当する 12.0 基づいたリリースがありません。		
Affected 12.1-Based Releases	First Fixed Release（修正された最初のリリース）	**推奨リリース**
該当する 12.1 基づいたリリースがありません。		
Affected 12.2-Based Releases	First Fixed Release（修正された最初のリリース）	**推奨リリース**
12.2	脆弱性なし	
12.2B	脆弱性なし	
12.2BC	脆弱性なし	
12.2BW	脆弱性なし	
12.2BX	脆弱性なし	
12.2BY	脆弱性なし	
12.2BZ	脆弱性なし	
12.2CX	脆弱性なし	
12.2CY	脆弱性なし	
12.2CZ	脆弱性なし	
12.2DA	脆弱性なし	
12.2DD	脆弱性なし	
12.2DX	脆弱性なし	
12.2EW	脆弱性なし	
12.2EWA	脆弱性なし	
12.2EX	脆弱性なし	
12.2EY	脆弱性なし	
12.2EZ	脆弱性なし	
12.2FX	脆弱性なし	
12.2FY	脆弱性なし	
12.2FZ	脆弱性なし	
12.2IRA	脆弱性なし	

12.2IRB	脆弱性なし	
12.2IRC	脆弱性なし	
12.2IXA	脆弱性なし	
12.2IXB	脆弱性なし	
12.2IXC	脆弱性なし	
12.2IXD	脆弱性なし	
12.2IXE	脆弱性なし	
12.2IXF	脆弱性なし	
12.2IXG	脆弱性なし	
12.2IXH	脆弱性なし	
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	
12.2MB	脆弱性なし	
12.2MC	脆弱性なし	
12.2S	脆弱性なし	
12.2SB	脆弱性なし	
12.2SBC	脆弱性なし	
12.2SCA	脆弱性なし	
12.2SCB	脆弱性なし	
12.2SE	脆弱性なし	
12.2SEA	脆弱性なし	
12.2SEB	脆弱性なし	
12.2SEC	脆弱性なし	
12.2SED	脆弱性なし	
12.2SEE	脆弱性なし	
12.2SEF	脆弱性なし	
12.2SEG	脆弱性なし	
12.2SG	脆弱性なし	
12.2SGA	脆弱性なし	
12.2SL	脆弱性なし	
12.2SM	脆弱性なし	
12.2SO	脆弱性なし	
12.2SQ	脆弱性なし	
12.2SRA	脆弱性なし	
12.2SRB	脆弱性なし	
12.2SRC	脆弱性なし	
12.2SRD	脆弱性なし	
12.2STE	脆弱性なし	
12.2SU	脆弱性なし	
12.2SV	脆弱性なし	
12.2SVA	脆弱性なし	
12.2SVC	脆弱性なし	

12.2SVD	脆弱性なし	
12.2SVE	脆弱性なし	
12.2SW	脆弱性なし	
12.2SX	脆弱性なし	
12.2SXA	脆弱性なし	
12.2SXB	脆弱性なし	
12.2SXD	脆弱性なし	
12.2SXE	脆弱性なし	
12.2SXF	脆弱性なし	
12.2SXH	脆弱性なし	
12.2SXI	脆弱性なし	
12.2SY	脆弱性なし	
12.2SZ	脆弱性なし	
12.2T	脆弱性なし	
12.2TPC	脆弱性なし	
12.2XA	脆弱性なし	
12.2XB	脆弱性なし	
12.2XC	脆弱性なし	
12.2XD	脆弱性なし	
12.2XE	脆弱性なし	
12.2XF	脆弱性なし	
12.2XG	脆弱性なし	
12.2XH	脆弱性なし	
12.2XI	脆弱性なし	
12.2XJ	脆弱性なし	
12.2XK	脆弱性なし	
12.2XL	脆弱性なし	
12.2XM	脆弱性なし	
12.2XNA	Cisco IOS XE ソフトウェア 可用性を参照して下さい	
12.2XNB	Cisco IOS XE ソフトウェア 可用性を参照して下さい	
12.2XNC	Cisco IOS XE ソフトウェア 可用性を参照して下さい	
12.2XND	Cisco IOS XE ソフトウェア 可用性を参照して下さい	
12.2XO	脆弱性なし	
12.2XQ	脆弱性なし	
12.2XR	脆弱性なし	
12.2XS	脆弱性なし	
12.2XT	脆弱性なし	
12.2XU	脆弱性なし	
12.2XV	脆弱性なし	

12.2XW	脆弱性なし	
12.2YA	脆弱性なし	
12.2YB	脆弱性なし	
12.2YC	脆弱性なし	
12.2YD	脆弱性なし	
12.2YE	脆弱性なし	
12.2YF	脆弱性なし	
12.2YG	脆弱性なし	
12.2YH	脆弱性なし	
12.2YJ	脆弱性なし	
12.2YK	脆弱性なし	
12.2YL	脆弱性なし	
12.2YM	脆弱性なし	
12.2YN	脆弱性なし	
12.2YO	脆弱性なし	
12.2YP	脆弱性なし	
12.2YQ	脆弱性なし	
12.2YR	脆弱性なし	
12.2YS	脆弱性なし	
12.2YT	脆弱性なし	
12.2YU	脆弱性なし	
12.2YV	脆弱性なし	
12.2YW	脆弱性なし	
12.2YX	脆弱性なし	
12.2YY	脆弱性なし	
12.2YZ	脆弱性なし	
12.2ZA	脆弱性なし	
12.2ZB	脆弱性なし	
12.2ZC	脆弱性なし	
12.2ZD	脆弱性なし	
12.2ZE	脆弱性なし	
12.2ZF	脆弱性なし	
12.2ZG	脆弱性なし	
12.2ZH	脆弱性なし	
12.2ZJ	脆弱性なし	
12.2ZL	脆弱性なし	
12.2ZP	脆弱性なし	
12.2ZU	脆弱性なし	
12.2ZX	脆弱性なし	
12.2ZY	脆弱性なし	
12.2ZYA	脆弱性なし	
Affected 12.3-	First Fixed Release (修正された最初のリリース)	**推奨リリース**

Based Releases		
該当する 12.3 基づいたリリースがありません。		
Affected 12.4-Based Releases	First Fixed Release (修正された最初のリリース)	**推奨リリース**
12.4	脆弱性なし	
12.4GC	脆弱性なし	
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JDC	脆弱性なし	
12.4JDD	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	12.4(15)MD3	12.4(15)MD3
12.4MDA	脆弱性なし	
12.4MR	12.4(19)MR3	12.4(19)MR3
12.4SW	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4
12.4T	12.4(15)T10 12.4(22)T2 12.4(20)T3 12.4(24)T	12.4(15)T10 12.4(20)T4
12.4XA	脆弱性なし	
12.4XB	脆弱性なし	
12.4XC	脆弱性なし	
12.4XD	脆弱性なし	
12.4XE	脆弱性なし	
12.4XF	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4
12.4XG	脆弱性なし	
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4
12.4XK	脆弱性あり; first fixed in 12.4T	12.4(1

		5)T10 12.4(20)T4
12.4XL	脆弱性なし	
12.4XM	脆弱性なし	
12.4XN	脆弱性なし	
12.4XP	脆弱性なし	
12.4XQ	12.4(15)XQ3	12.4(15)T10
12.4XR	12.4(15)XR5	12.4(15)XR7 12.4(22)XR
12.4XT	脆弱性なし	
12.4XV	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.4XW	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4
12.4XY	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4
12.4XZ	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4
12.4YA	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4
12.4YB	脆弱性なし	
12.4YD	脆弱性なし	
12.4YE	脆弱性なし	

注: Cisco IOSソフトウェア モジュール性リリースはこの脆弱性から影響を受けしません。

Cisco IOS XE ソフトウェア

IOS XE リリース	First Fixed Release (修正された最初のリリース)
2.1.x	脆弱性なし
2.2.x	脆弱性なし

2.3.x	2.3.2
2.4.x	脆弱性なし

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

この脆弱性は内部テストで発見されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls

改訂履歴

リビジョン 1.0	2009-September-23	初版リリース

利用規約