Cisco IOSソフトウェアにおける巧妙に細工された暗号化パケットによるDenial of Service(DoS)の脆弱性

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 IOS®ソフトウェアには、攻撃者が巧妙に細工された暗号化パケットをリモートから送信することで、Cisco IOSデバイスをリロードさせる可能性のある脆弱性が存在します。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls で公開されています。

注：2009年9月23日のCisco IOSセキュリティ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。

個々の公開リンクは、次のリンクの「Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication」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

該当するバージョンのCisco IOSソフトウェアを実行しているデバイスは、次のいずれかの機能が設定されている場合に影響を受けやすくなります。

- Secure Socket Layer(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)暗号化ナンス

注：WebVPNおよびSSL VPN以外のSSL/HTTPS関連機能は、この脆弱性の影響を受けません。

デバイスでSSLVPNが有効になっているかどうかを確認するには、デバイスにログインして、コマンドラインインターフェイス(CLI)コマンドshow running-config | include webvpnコマンドを使用します。デバイスから何らかの出力が返された場合、SSLVPNが設定されており、そのデバイスには脆弱性が存在する可能性があります。脆弱性のある設定は、デバイスがCisco IOS WebVPN(リリース12.3(14)Tで導入)またはCisco IOS SSLVPN(リリース12.4(6)Tで導入)のどちらをサポートしているかによって異なります。次に、デバイスに脆弱性が存在するかどうかを確認する方法を示します。

「show running-config | include webvpn」に「webvpn enable」が含まれている場合、デバイスは元のCisco IOS WebVPNで設定されています。デバイスが脆弱かどうかを判断する唯一の方法は、「show running-config」の出力を調べて、webvpnがコマンド「webvpn enable」によって有効になっており、「ssl trustpoint」が設定されていることを確認することです。次の例は、Cisco IOS WebVPNが設定された脆弱性のあるデバイスを示しています。

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

「show running-config | include webvpn」に「webvpn gateway <word>」が含まれている場合、デバイスはCisco IOS SSLVPN機能をサポートしています。「webvpn gateway」セクションの少なくとも1つに「inservice」コマンドがあるデバイスは脆弱です。次の例は、Cisco IOS SSLVPNが設定された脆弱性のあるデバイスを示しています。

<#root>

```
Router#
```

show running | section webvpn

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

Cisco IOS SSLVPNをサポートするデバイスで「webvpn gateways」が設定されていない場合、または設定されているすべての「webvpn gateways」に「no inservice」webvpn gatewayコマンドが含まれている場合は、この脆弱性は存在しません。

SSHが有効になっているかどうかを確認するには、次の例に示すようにshow ip sshコマンドを使用します。

```
<#root>

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暗号化ナンス機能が有効になっているかどうかを確認するには、show running-config | include rsa-encrコマンドを次に示します。

```
<#root>

Router#

show running-config | inc rsa-encr

 authentication rsa-encr
```

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て show version コマンドを使って、システム バナーを表示します。"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。他のシスコ デバイスでは、show version コマンドが存在しなかったり、別の出力が表示されたりします。

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:

```
<#root>

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、インストールされたイメージ名が C1841-ADVENTERPRISEK9-M で、Cisco IOS ソフトウェア リリース 12.4(20)T を実行しているシスコ製品を示しています。

```
<#root>

Router#

show version

Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc
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ソフトウェアリリースの命名規則の追加情報は、次のリンクの「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の影響を受けません。

Cisco IOS XRソフトウェアは、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またはSSHが設定されたCisco IOSデバイスは、TCPポート443(SSLVPN)またはTCPポート22(SSH)で特別に巧妙に細工されたTCPパケットを受信すると、リロードする可能性があります。この脆弱性を不正利用するには、これらの機能に関連付けられたTCPポート番号に対する3ウェイハンドシェイクを完了する必要があります。ただし、認証は必要ありません。IKE暗号化ナンス用に設定されたCisco IOSデバイスは、ポート500または4500(NAT Traversal(NAT-T)用に

設定されている場合)で特別に巧妙に細工されたUDPパケットを受信すると、リロードする可能性があります。

この脆弱性は、Cisco Bug ID CSCsq24002 (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-2871が割り当てられています。

回避策

影響を受ける機能を無効にし、VTYアクセスコントロールリストを使用してSSHアクセスを保護する以外に、使用可能な回避策はありません。

no webvpn enableコマンドを使用して、SSL VPNの使用を無効にします。

Cisco IOSでは、コンフィギュレーションモードでコマンドcrypto key zeroize rsaを適用することでSSHサーバを無効にできます。SSHサーバは、RSAキーペアの生成時に自動的に有効になります。RSAキーをゼロにすることは、SSHサーバを完全に無効にする唯一の方法です。

Cisco IOSソフトウェア上のSSHサーバへのアクセスも、有効なトランスポートプロトコルとしてSSHを削除することで無効にできます。このアクションを実行するには、コンフィギュレーションモードで、vty回線上の許可されたトランスポートのリストから「ssh」を削除した状態でtransport inputコマンドを再適用します。例：

```
line vty 0 4
      transport input telnet
    end
```

SSHサーバ機能が必要な場合は、次のURLに示すように、vty回線のアクセスコントロールリスト(ACL)を使用して、サーバへのアクセスを特定の送信元IPアドレスに制限するか、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の設定の詳細については、シスコのパブリックWebサイトを参照してください。

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

vtyアクセスリストの例を次に示します。

```
access-list 2 permit 10.1.1.0 0.0.0.255
access-list 2 deny any

line vty 0 4
 access-class 2 in
```

前の例では、10.1.1.0/24ネットワークだけがCisco IOSデバイスへのSSHを許可されています。

IKE暗号化ナンスを無効にするには、次の例に示すように、ISAKMPポリシーでno authentication rsa-encrコマンドを使用します。

```
crypto isakmp policy
 no authentication rsa-encr
```

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード 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ベースのリリースはありません。		

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ベースのリリースはありません。		

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 ソフトウェアの可用性を参照してください。	
12.2XNB	Cisco IOS XE ソフトウェアの可用性を参照してください。	
12.2XNC	Cisco IOS XE ソフトウェアの可用性を参照してください。	
12.2XND	Cisco IOS XE ソフトウェアの可用性を参照してください。	
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-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12.3ベースのリリースはありません。		
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(最初の修正は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(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4

12.4XG	脆弱性なし	
12.4XJ	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4
12.4XK	脆弱性あり(最初の修正は12.4T)	12.4(15)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の取得」セクションの手順に従って、サポート組織にお問い合わせください	
12.4XW	脆弱性あり(最初の修正は12.4T)	12.4(15)T10

		12.4(20)T4
12.4XY	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4
12.4XZ	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4
12.4YA	脆弱性あり(最初の修正は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：この脆弱性の影響を受けるCisco IOS Software Modularityリリースはありません。

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

推奨事項

$propertyAndFields.get("recommendations")

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やその公表は確認しておりません。

この脆弱性は内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls

改訂履歴

リビジョン 1.0	2009年9月23日	初版リリース

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。