Cisco IOSソフトウェア Internet Key Exchange（IKE）リソース の 枯渇脆弱性

High

アドバイザリーID : cisco-sa-20090923-ipsec

初公開日 : 2009-09-23 16:00

バージョン 1.2 : Final

CVSSスコア : 7.8

回避策 : No Workarounds available

Cisco バグ ID : CSCsy07555

CVE-2009-2868

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

インターネット キー エクスチェンジ（IKE）プロトコルおよび認証ベースの認証のために設定される Cisco IOS® デバイスはリソース の 枯渇 攻撃に脆弱です。 この脆弱性の不正利用の成功はすべての利用可能 なフェーズ 1 Security Associations （SA）のアロケーションという結果に終り、新しい IPSecセッションの確立を防ぐかもしれません。

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-ipsec 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

IKE および認証ベースの認証のために影響を受けている設定される Cisco IOSデバイス、デバイスの RSA キーがある場合。

脆弱性のある製品

IKE は IPsec が使用される場合デフォルトで有効に なります。 IKE のために設定される Cisco IOSデバイスは UDP ポート 500、UDP ポート 4500、または UDP ポート 848 または 4848 でデバイスがグループ ドメイン オブ インタープリテーション (GDOI) のために設定される場合デバイスが NAT 走査 (NAT-T) のために設定されれば受信します。 UDP ポート 500 で受信しているルータを以下に示します:

```
Router#show ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
....
 17   --listen--          192.168.66.129    500   0   0   11   0
....
```

または

```
Router-#show udp
Proto        Remote      Port      Local       Port  In Out  Stat TTY OutputIF
 17       --listen--          192.0.2.1         500   0   0  1011   0
 17(v6)   --listen--          --any--           500   0   0 20011   0
Router#
```

IKE コンフィギュレーションは show crypto isakmp policy コマンドの出力の認証方式として認証によって基づく認証を行っている Rivest-Shamir-Adleman シグニチャを表示する。 この出力は次の例で示されています:

```
Router#show crypto isakmp policy

Global IKE policy
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

show crypto key mypubkey rsa コマンドがシステムの RSA キーがあるかどうか確認するのに使用することができます。 この出力は次の例で示されています:

```
Router#show crypto key mypubkey rsa
% Key pair was generated at: 06:07:49 UTC Jan 13 1996
Key name: myrouter.example.com
  Usage: Signature Key
  Key Data:
   005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B
   55D6AB22
   04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C
   73A05DD2
   BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

% Key pair was generated at: 06:07:50 UTC Jan 13 1996
Key name: myrouter.example.com
```

```
Usage: Encryption Key
Key Data:
 00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748
 429618D5
 18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD
 9A8A26DB
 07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 "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。

次の例は s72033_rp-IPSERVICESK9_WAN-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 12.2(18)SXF7 を実行している Cisco 6500 シリーズ デバイスを識別したものです:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-IPSERVICESK9_WAN-M), Version 12.2(18)SXF7, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright Â©) 1986-2006 by cisco Systems, Inc.
Compiled Thu 23-Nov-06 06:42 by kellythw
<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 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

IPsec は IP パケットの強い認証および暗号化を提供する IPセキュリティ 機能です。 IKE は IPsec 規格と共に使用するキー管理プロトコル規格です。

IKE は Internet Security Association and Key Management Protocol（ISAKMP）フレームワークの中の Oakley および SKEME 鍵交換を設定するハイブリッド プロトコルです。（ISAKMP、Oakley および SKEME は IKE によって。設定される）セキュリティプロトコルです。 IKE の次のリンクを参照して下さい:

http://www.cisco.com/en/US/docs/ios/12_1/security/configuration/guide/scdike.html

認証ベースの認証認証方法が使用される場合 Cisco IOSソフトウェアの IKE 実装で存在 する脆弱性。 この脆弱性の不正利用の成功は新しい IPSecセッションは確立されることを防ぐかもしれないすべての利用可能 なフェーズ 1 SA のアロケーションという結果に終るかもしれません。

不正利用の結果として **show crypto isakmp sa コマンドの**発行によって割り当てられる管理者はフェーズ 1 SA を表示できます。 次の例はこのコマンドのための出力例を表示するものです:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.48.66.77     10.48.66.6      MM_KEY_EXCH       1004 ACTIVE
10.48.66.77     10.48.66.6      MM_KEY_EXCH       1003 ACTIVE
10.48.66.77     10.48.66.6      MM_KEY_EXCH       1002 ACTIVE
....
```

どの割り当てられた SA でも手動での上で **clear crypto isakmp の**使用によって <conn **ID >** コマンド割り当て解除することができます。

この脆弱性 Cisco バグ ID **CSCsy07555** （登録ユーザのみ）および **CSCee72997** （登録ユーザのみ）によって当たり、よくある脆弱性および公開（CVE）ID CVE-2009-2868 は割り当てられました。

回避策

RSA キーがシステムで必要とされない場合、**crypto key zeroize rsa コマンドが**システムからすべての RSA キーを削除するのに使用することができます。 これが RSA キーを使用しているセキュア シェル（SSH）を含むすべての機能を壊すことに注目して下さい。

ネットワークの on Cisco 配置されたデバイスの場合もある追加軽減は次のリンクで利用可能のこのアドバイザリに Cisco によって加えられる軽減情報ドキュメントガイドで利用できます、:
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090923-ipsec

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 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	Release prior to 12.2(44)EX are vulnerable， releases 12.2(44)EX and later are not vulnerable;	12.2(50)SE3 12.2(52)S

	migrate to any release in 12.2SEG	E; 13-OCT-2009 で利用可能
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	脆弱性あり; first fixed in 12.2SRD	12.2(33)SRD3
12.2IRB	脆弱性あり; first fixed in 12.2SRD	12.2(33)SRD3
12.2IRC	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	
12.2IXA	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	12.2(33)SB6	12.2(31)SB16 12.2(33)SB7
12.2SBC	脆弱性なし	
12.2SCA	脆弱性あり; first fixed in 12.2SCB	12.2(33)SCB4
12.2SCB	12.2(33)SCB4	12.2(33)SCB4
12.2SE	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能	12.2(50)SE3 12.2(52)SE; 13-OCT-2009

		で利用可能
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	脆弱性あり; first fixed in 12.2SRD	12.2(33)SRD3
12.2SRB	脆弱性あり; first fixed in 12.2SRD	12.2(33)SRD3
12.2SRC	12.2(33)SRC5; 29-OCT-2009 で利用可能	12.2(33)SRD3
12.2SRD	12.2(33)SRD3 12.2(33)SRD2a	12.2(33)SRD3
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	
12.2SX	脆弱性なし	

A		
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	12.2(33)SXH6; 30-OCT-2009 で利用可能 IOS software モジュール性パッチを参照して下さい	12.2(33)SXH6; 30-OCT-2009 で利用可能
12.2SXI	12.2(33)SXI2a	12.2(33)SXI2a
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-Based Releases	First Fixed Release（修正された最初のリリース）	推奨リリース
12.3	脆弱性なし	
12.3B	脆弱性なし	
12.3BC	脆弱性なし	
12.3BW	脆弱性なし	
12.3EU	脆弱性なし	
12.3JA	脆弱性なし	
12.3JEA	脆弱性なし	
12.3JEB	脆弱性なし	
12.3JEC	脆弱性なし	
12.3JK	脆弱性なし	
12.3JL	脆弱性なし	
12.3JX	脆弱性なし	
12.3T	脆弱性あり; first fixed in 12.4 12.3(8)T11 以前のリリースは脆弱ではないです。	12.4(25b) 12.4(23b)
12.3TPC	脆弱性なし	
12.3VA	脆弱性なし	
12.3XA	脆弱性なし	
12.3XB	脆弱性なし	
12.3XC	脆弱性なし	
12.3XD	脆弱性なし	
12.3XE	脆弱性なし	
12.3XF	脆弱性なし	
12.3XG	脆弱性なし	
12.3XI	脆弱性なし	
12.3XJ	脆弱性なし	
12.3XK	脆弱性なし	
12.3XL	脆弱性あり; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-

		OCT-2009 で利用可能
12.3XQ	脆弱性なし	
12.3XR	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XS	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XU	脆弱性なし	
12.3XW	脆弱性なし	
12.3XX	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XY	脆弱性なし	
12.3XZ	脆弱性なし	
12.3YA	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3YD	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YF	脆弱性あり; migrate to any release in 12.4XN	12.4(15)XR7 12.4(22)XR
12.3YG	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YH	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-

		OCT-2009 で利用可能
12.3YI	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YJ	脆弱性なし	
12.3YK	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YM	脆弱性なし	
12.3YQ	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YS	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(15)T10

		12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YU	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YX	脆弱性あり; migrate to any release in 12.4XN	12.4(15)XR7 12.4(22)XR
12.3YZ	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	
12.3ZA	脆弱性なし	
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	12.4(7) 以前のリリースは脆弱です; リリース 12.4(7a) およびそれ以降は脆弱ではないです。	12.4(25b) 12.4(23b)
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	脆弱性なし	
12.4MDA	脆弱性なし	
12.4MR	脆弱性なし	
12.4SW	脆弱性なし	
12.4T	12.4(4)T8 12.4(9)T 12.4(6)T1	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XB	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XC	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可

		能
12.4XD	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XE	脆弱性なし	
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性なし	
12.4XK	脆弱性なし	
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	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性なし	
12.4XV	脆弱性なし	
12.4XW	脆弱性なし	
12.4XY	脆弱性なし	
12.4XZ	脆弱性なし	
12.4YA	脆弱性なし	
12.4YB	脆弱性なし	
12.4YD	脆弱性なし	
12.4YE	脆弱性なし	

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
2.1.x	2.3.0t
2.2.x	2.3.0t
2.3.x	脆弱性なし
2.4.x	脆弱性なし

Cisco IOSソフトウェア モジュール性-メンテナンス パック

Cisco IOS Software Modularity をご使用のお客様は、個別のメンテナンス パックを適用できます。 Cisco IOS Software Modularity についての追加情報は以下のリンクをご参照下さい: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd80313e15.html

下記に記載されているメンテナンス パックは http://www.cisco.com/go/pn でダウンロードすることができます

12.2SXH のための Cisco IOSソフトウェア モジュール性メンテナンス パック

Cisco IOS ソフトウェア リリース	ソリューション メンテナンス Pack (MP)
12.2(33)SXH5	MP001

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、お客様 によって Cisco に報告されました。

出典

URL

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

改訂履歴

リビジョン 1.2	2009-October-19	更新済イオン ソフトウェア テーブル。
リビジョン 1.1	2009-October-02	対応策として追加された crypto key zeroize rsa コマンド。
リビジョン 1.0	2009-September-23	初版リリース

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な

情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。