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)リソース枯渇の脆弱性

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)プロトコルおよび証明書ベースの認証が設定されているCisco IOS®デバイスは、リソース枯渇攻撃に対して脆弱です。この脆弱性の不正利用に成功すると、使用可能なすべてのフェーズ1セキュリティアソシエーション(SA)が割り当てられ、新しいIPSecセッションの確立が妨げられる可能性があります。

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-ipsec 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

IKEおよび証明書ベースの認証用に設定されたCisco IOSデバイスは、デバイスにRSAキーが存在する場合に影響を受けます。

脆弱性のある製品

IPsec を使用している場合、IKE はデフォルトで有効になっています。IKE 用に設定されている Cisco IOS デバイスは、デバイスが NAT トラバーサル（NAT-T）用に設定されている場合は UDP ポート 500 または 4500 をリッスンし、デバイスが Group Domain of Interpretation（GDOI; グループ ドメイン オブ インタープリテーション）用に設定されている場合は UDP ポート 848 または 4848 をリッスンします。次の出力は、UDP ポート 500 をリッスンしているルータを示しています。

<#root>

```
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

<#root>

```
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#
```

証明書ベースの認証を実行しているIKE設定では、show crypto isakmp policyコマンドの出力に、認証方式としてRivest-Shamir-Adleman Signatureと表示されます。この出力を次の例に示します。

<#root>

```
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コマンドを使用すると、システムにRSAキーが存在するかどうかを確認できます。この出力を次の例に示します。

<#root>

```
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。

次の例は、Cisco 6500シリーズデバイスでCisco IOSソフトウェアリリース12.2(18)SXF7が稼働し、インストールされているイメージ名がs72033_rp-IPSERVICESK9_WAN-Mであることを示しています。

<#root>

```
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 (
Technical Support: http://www.cisco.com/techsupport
Copyright ©) 1986-2006 by cisco Systems, Inc.
Compiled Thu 23-Nov-06 06:42 by kellythw
<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 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

IPsec は、IP パケットに対して強力な認証や暗号化を実現する IP セキュリティ機能です。IKEは、IPSec標準と組み合わせて使用されるキー管理プロトコル標準です。

IKE は、Oakley キー交換や Skeme キー交換を Internet Security Association and Key Management Protocol（ISAKMP）フレームワーク内に実装するハイブリッド プロトコルです（ISAKMP、Oakley、および Skeme は、IKE により実装されるセキュリティ プロトコルです）。IKE の詳細については、次のリンクを参照してください。

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

証明書ベースの認証方式を使用している場合、Cisco IOSソフトウェアのIKE実装には脆弱性が存在します。この脆弱性の不正利用に成功すると、利用可能なすべてのフェーズ1 SAの割り当てが発生し、新しいIPSecセッションの確立が妨げられる可能性があります。

管理者は、show crypto isakmp saコマンドを発行することで、不正利用によって割り当てられたフェーズ1 SAを表示できます。次の例は、このコマンドの出力例を示しています。

```
<#root>

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
....
```

clear crypto isakmp <conn-ID>コマンドを使用すると、割り当て済みのすべてのSAの割り当てを手動で解除できます。

この脆弱性は、Cisco Bug ID CSCsy07555（登録ユーザ専用）およびCSCee72997(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-2009-2868が割り当てられています。

回避策

RSAキーがシステムで必要ない場合は、crypto key zeroize rsaコマンドを使用して、システムからすべてのRSAキーを削除できます。これにより、セキュアシェル(SSH)を含む、RSAキーを使用しているすべての機能が無効になります。

ネットワーク内のCiscoデバイスに適用可能な他の対応策は、このアドバイザリに関連するCisco適用対応策速報を次のリンク先で参照できます。https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090923-ipsec

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	12.2(44)EXより前のリリースには脆弱性があり、12.2(44)EX以降のリリースには脆弱性はありません。 12.2SEGの任意のリリースに移行してください。	12.2(50)SE3 12.2(52)SE（2009年10月13日に入手可能）
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(最初の修正は12.2SRD)	12.2(33)SRD3
12.2IRB	脆弱性あり(最初の修正は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	
12.2IXA	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(最初の修正は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（2009年10月13日に入手可能）	12.2(50)SE3 12.2(52)SE（2009年10月13日に入手可能）
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(最初の修正は12.2SRD)	12.2(33)SRD3
12.2SRB	脆弱性あり(最初の修正は12.2SRD)	12.2(33)SRD3
12.2SRC	12.2(33)SRC5（2009年10月29日に入手可能）	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	
12.2SXA	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	12.2(33)SXH6（2009年10月30日に入手可能） 「IOS Software Modularity Patch」を参照してください。	12.2(33)SXH6（2009年10月30日に入手可能）

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

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(最初の修正は12.4) 12.3(8)T11までのリリースには脆弱性はありません。	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(最初の修正は12.4T)	12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3XQ	脆弱性なし	
12.3XR	脆弱性あり(最初の修正	12.4(25b)

	は12.4)	12.4(23b)
12.3XS	脆弱性あり(最初の修正は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(最初の修正は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(最初の修正は12.4)	12.4(25b) 12.4(23b)
12.3YD	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3YF	脆弱性あり。12.4XNの任意のリリースに移行	12.4(15)XR7 12.4(22)XR
12.3YG	脆弱性あり(最初の修正	12.4(15)T10

	は12.4T)	12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3YH	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3YI	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3YJ	脆弱性なし	
12.3YK	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3YM	脆弱性なし	
12.3YQ	脆弱性あり(最初の修正は12.4T)	12.4(15)T10

		12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3YS	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3YT	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3YU	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.3YX	脆弱性あり。12.4XNの任意のリリースに移行	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	
12.3ZA	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)より前のリリースには脆弱性があり、12.4(7a)以降のリリースには脆弱性はありません。	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（2009年10月23日に入手可能）
12.4XA	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.4XB	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）

12.4XC	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
12.4XD	脆弱性あり(最初の修正は12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2（2009年10月23日に入手可能）
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 Software Modularity – 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の詳細については、次のリンクを参照してください。http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd80313e15.html

下記のメンテナンスパックは、http://www.cisco.com/go/pnからダウンロードできます。

12.2SXH用Cisco IOS Software Modularity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パック(MP)
12.2(33)SXH5	MP001

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、お客様からシスコに報告されたものです。

URL

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

改訂履歴

リビジョ	2009年10月	IONソフトウェアの表を更新。

ン 1.2	19日	
リビジョン 1.1	2009年10月2日	回避策としてcrypto key zeroize rsaコマンドを追加。
リビジョン 1.0	2009年9月23日	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。

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。