暗号ライブラリの脆弱性

High

アドバイザリーID : cisco-sa-20070522-crypto
初公開日 : 2007-05-22 13:00
バージョン 2.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCsd85587

CVE-2006-3894

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

多くの Cisco 製品で使用されているサードパーティ製の暗号ライブラリで、脆弱性が発見されました。この脆弱性は、不正形式の Abstract Syntax Notation One（ASN.1）オブジェクトが解析されたときに、トリガーされる可能性があります。この脆弱性の性質上、場合によっては、有効な証明書または有効なアプリケーション層クレデンシャル（有効なユーザ名とパスワードなど）がなくても、この脆弱性がトリガーされる可能性があります。

これらの脆弱性が繰り返し悪用されると、持続的な Denial-of-Service（DoS; サービス拒否）が発生する可能性があります。ただし、これらの脆弱性によってデータやサービスの機密性または整合性が損なわれるかどうかは不明です。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。

脆弱性のある暗号ライブラリは、次の Cisco 製品で使用されています。

- Cisco IOS
- Cisco IOS XR
- Cisco PIX および ASA セキュリティ アプライアンス
- Cisco Firewall Service Module（FWSM）
- Cisco Unified CallManager

この脆弱性には、CVE ID CVE-2006-3894 が割り当てられています。この脆弱性への対応は Cisco の外部で管理されており、次の外部コーディネータによって追跡されています。

- JPCERT/CC - JVNVU#754281 として追跡
- CPNI - NISCC-362917 として追跡
- CERT/CC - VU#754281 として追跡

シスコでは、該当するお客様用に、こ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

。この脆弱性に対しては、影響を緩和するための回避策が存在しません。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto で公開されています。

注：このアドバイザリとともに、関連する別のアドバイザリが公開されています。そのアドバイザリでは、Cisco IOS に影響を与える暗号関連の脆弱性が説明されています。関連するアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL で公開されています。

該当製品

脆弱性のある製品

この脆弱性には、該当するバージョンのサードパーティ暗号ライブラリを使用するすべての製品、および暗号関連機能を使用する有効なアプリケーションが該当します。次の Cisco 製品には脆弱性が含まれていることが確認されています。

- Cisco IOS
- Cisco IOS XR
- Cisco PIX および ASA セキュリティ アプライアンス（該当するのは 7.x リリースのみ）
- Cisco Firewall Service Module（FWSM）（該当するのは 3.1(6) より前のリリースのみ。2.3(x) リリースは該当しません）
- Cisco Unified CallManager

次に示すアプリケーション層プロトコルまたは機能を有効にすると、デバイスはこの脆弱性に該当します。いずれか 1 つのプロトコルまたは機能を有効にするだけで、デバイスはこの脆弱性に該当します。この脆弱性に該当しないようにするには、次に示されているすべてのアプリケーション プロトコルまたは機能を無効にする必要があります。

Cisco IOS で該当するプロトコル

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。

```
<#root>

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リリースの命名方法の詳細については、次のリンクを参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/
products_white_paper09186a008018305e.shtml

この脆弱性に該当する IOS ソフトウェア リリースが稼働している場合、次のプロトコルまたは機能のいずれか 1 つでも有効にすると、この脆弱性に該当します。

- Internet Security Association and Key Management Protocol（ISAKMP）
- 一部の IOS リリースでは、Secure Socket Layer（SSL）も該当する可能性があります。
- Threat Information Distribution Protocol（TIDP）
- Cisco IOS SIP Gateway Signaling Support Over TLS（SIP-TLS）
- Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）

他のプロトコルの中にも該当する暗号ライブラリを使用しているものが含まれる可能性があるので、自分の IOS リリースが脆弱かどうかを判定する最も正確な方法は、修正済み IOS リリースの表を調べることです。

Internet Security Association and Key Management Protocol（ISAKMP）

暗号マップを明示的に設定してインターフェイスに適用すると、IOS デバイスが脆弱になります。すべての認証方法（つまり、事前共有キー、証明書）が該当します。

特定のデバイスで ISAKMP が有効になっているかどうかを確認するには、show crypto isakmp policy コマンドを入力します。ISAKMP が有効になっているデバイスの例を次に示します。

```
<#root>
```

```
Router#
show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
<more output>
```

次の例のような出力が表示された場合、そのデバイスでは IKE が有効になっていません。

```
<#root>
Router#
show crypto isakmp policy
ISAKMP is turned off
```

Cisco IOS では、2 つの機能が ISAKMP - IPSec および Group Domain of Interpretation（GDOI）に依存しています。前の例では、これらの機能のどちらが存在していても検出されます。

IOS バージョン 12.3(2)T より前のリリースでは、IKE がデフォルトで有効になっているため、IOS デバイスが IKE メッセージを処理するための暗号設定は必要ありませんでした。

Cisco IOS の 12.2SXD バージョンでは、IKE がデフォルトで有効になっています。IKE 処理を確実に無効にするには、グローバル設定コマンド no crypto isakmp enable を入力します。

IOS バージョン 12.3(2)T（すべての 12.4 ベース バージョンを含む）で IKE メッセージ処理を有効にするには、暗号設定が必要です。

Secure Socket Layer (SSL)

Cisco IOS ソフトウェアの一部のリリースでは、SSL 機能の要素を処理するために、脆弱なライブラリが使用されています。SSL は、Hyper Text Transfer Protocol over SSL（HTTPS）などのアプリケーション層プロトコルを保護するために使用されます。

HTTPS は、SSL を使用する可能性のある唯一のプロトコルではありませんが、最もよく知られているものです。デバイスでHTTPSが設定されているかどうかを確認するには、`show running`コマンドを入力します。 `| include secure`コマンドを使用します。HTTPS が有効になっているデバイスの例を次に示します。

```
<#root>
router#
```

```
show running | include secure-server
ip http secure-server
```

Threat Information Distribution Protocol（TIDP）

デバイスでTDIPが有効になっているかどうかを確認するには、`show running-config`コマンドを入力します。 `| include parameter-map`コマンドを使用します。TDIP が有効になっているデバイスの例を次に示します。

```
<#root>
router#
show running | include parameter-map
parameter-map type tms TMS_PAR
```

Cisco IOS SIP Gateway Signaling Support Over TLS（SIP-TLS）

デバイスでSIP-TLSが有効になっているかどうかを確認するには、`show running-config`コマンドを入力します。 `| include crypto signaling`コマンドを使用します。SIP-TLS が有効になっているデバイスの例を次に示します。

```
<#root>
router#
show running | include crypto signaling
crypto signaling default trustpoint user1
```

Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）

デバイスでEAP-TLSが有効になっているかどうかを確認するには、`show running-config`コマンドを入力します。 `| include`メソッドを使用します。EAP-TLS が有効になっているデバイスの例を次に示します。

```
<#root>
Router#
show running | include method
method tls
```

Cisco IOS XR で該当するプロトコル

この脆弱性に該当する Cisco IOS XR ソフトウェア リリースが稼働している場合、次のプロトコルまたは機能のいずれか 1 つでも有効にすると、この脆弱性に該当します。

- Internet Security Association and Key Management Protocol（ISAKMP）
- 一部の IOS XR リリースでは、Secure Socket Layer（SSL）も該当する可能性があります。
- セキュア シェル（SSH）

IOS XR の場合、脆弱性の悪用に成功してもデバイス全体がクラッシュすることはなく、該当するサービスのみがクラッシュします。この脆弱性が繰り返し悪用されると、デバイス全体ではなく、該当するサービスが持続的な DoS 状態になる可能性があります。

Internet Security Association and Key Management Protocol（ISAKMP）

デバイスでISAKMPが有効になっているかどうかを確認するには、`show running-config`コマンドを入力します。 `| include isakmp`コマンドを使用します。IKE が有効になっているデバイスの例を次に示します。

```
<#root>

Router#

show running-config | include isakmp


       crypto isakmp
       crypto isakmp policy 1
       crypto isakmp profile profile-a
```

Secure Socket Layer (SSL)

SSL は、Hyper Text Transfer Protocol over SSL（HTTPS）や Object Request Brokers（ORB; オブジェクト リクエスト ブローカ）などのアプリケーション層プロトコルで安全な通信を行うために使用されます。デバイスでSSLを使用するサービスが有効になっているかどうかを確認するには、次のコマンドのいずれかを入力します。`show running-config | | include http server ssl`または`show running-config | include xml agent corba ssl`コマンドを使用します。両方のサービスが有効になっているデバイスの例を次に示します。

```
<#root>

Router#

show running-config | include http server ssl
```

```
       http server ssl

Router#

show running-config | include xml agent corba ssl

       xml agent corba ssl
```

セキュア シェル（SSH）

SSH は、rsh、rlogin、rcp などの Berkeley r-tools スイートの代わりとなる安全な機能を提供するアプリケーションおよびプロトコルです。Telnet で対話形式のセッションを行う場合に好んで使用されます。デバイスでSSHが有効になっているかどうかを確認するには、`show running-config`コマンドを入力します。 `| include ssh server`コマンドを使用します。SSH が有効になっているデバイスの例を次に示します。

```
<#root>

Router#

show running-config | include ssh server

       ssh server
       ssh server rate-limit 100
```

Cisco PIX および ASA セキュリティ アプライアンスで該当するプロトコル

この脆弱性に該当する Cisco PIX および ASA ソフトウェア リリースが稼働している場合、次のプロトコルまたは機能のいずれか 1 つでも有効にすると、この脆弱性に該当します。

- セキュア シェル（SSH）
- Internet Security Association and Key Management Protocol（ISAKMP）
- Secure Socket Layer (SSL)

セキュア シェル（SSH）

特定のデバイスで SSH が有効になっているかどうかを確認するには、show running コマンドを入力し、出力を確認します。次の例のような行が含まれる場合は、SSH が有効になっています。

```
<#root>

PIX#

show running

....
```

```
ssh <host_IP_address> <host_netmask> <interface>
....
```

Internet Security Association and Key Management Protocol（ISAKMP）

特定のデバイスで ISAKMP が有効になっているかどうかを確認するには、show running コマンドを入力し、出力を確認します。次の例のような行が含まれる場合は、ISAKMP が有効になっています。

```
<#root>

PIX#

show running

....
crypto isakmp policy 2
 authentication rsa-sig
....
```

Secure Socket Layer (SSL)

SSL は、Hyper Text Transfer Protocol over SSL（HTTPS）や Cisco Adaptive Security Device Manager（ASDM）セッションなどのアプリケーション層プロトコルを保護するために使用されます。

特定のデバイスで SSL が有効になっているかどうかを確認するには、show running コマンドを入力し、出力を確認します。次の例のような行が含まれる場合は、SSL が有効になっています。

```
<#root>

PIX#

show running

....
http server enable
....
```

Cisco Firewall Service Module（FWSM）で該当するプロトコル

この脆弱性に該当する Cisco FWSM ソフトウェア リリースが稼働している場合、次のプロトコルまたは機能を有効にすると、この脆弱性に該当します。

- Internet Security Association and Key Management Protocol（ISAKMP）

Internet Security Association and Key Management Protocol（ISAKMP）

特定のデバイスで ISAKMP が有効になっているかどうかを確認するには、show running コマンドを入力し、出力を確認します。次の例のような行が含まれる場合は、ISAKMP が有効になっています。

```
<#root>

PIX#

show running

....
isakmp enable <interface-name>
....
```

Cisco Unified CallManager で該当するプロトコル

この脆弱性に該当する Cisco Unified CallManager ソフトウェア リリースが稼働している場合、次のプロトコルまたは機能のいずれか 1 つでも有効にすると、この脆弱性に該当します。

- Certificate Authority Proxy Function（CAPF）
- Cisco TAPI Service Provider（Cisco Unified CallManager TSP）

Certificate Authority Proxy Function（CAPF）

CAPF は Cisco CallManager とともに自動的にインストールされますが、デフォルトでは無効になっています。Unified CallManager で CAPF が有効になっているかどうかを確認するには、次の手順を実行します。

- ステップ 1：Cisco CallManager Administration で、Service > Service Parameter を選択します。
- 4.x ソフトウェアが稼働している場合は、Server ドロップダウン リスト ボックスから、パブリッシャ データベース サーバを選択します。5.x ソフトウェアが稼働している場合は、Server ドロップダウン リスト ボックスから、最初のノードを選択します。
- ステップ 3：Service ドロップダウン リスト ボックスから、Cisco Certificate Authority Proxy Function サービスを選択します。

CAPF パラメータが表示される場合は、CAPF がシステム上で稼働しています。

Cisco TAPI Service Provider（Cisco Unified CallManager TSP）

Cisco Unified CallManager TSP がインストールされているかどうかを確認するには、

Windows のコントロール パネルを開き（Start > Control Panel）、Add/Remove Programs をクリックします。「Cisco Unity-CM TSP」が一覧に表示される場合は、システムにインストールされています。

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。具体的には、次の製品機能および製品は該当しないことが判明しています。

- Cisco IOS
  - セキュア シェル（SSH）
  - Secure Copy（SCP）
- Cisco Unified Call Manager
  - Hyper Text Transfer Protocol over SSL（HTTPS）
  - Cisco Unified CallManager は、Secure Survivable Remote Site Telephony（SRST）を使用するように設定されます。
- MeetingPlace Express および MeetingPlace for Telepresence
- Cisco IP Communicator
- すべての Cisco Unified IP Phone 7900 シリーズ
- CIP TN3270 Server
- Cisco GSS 4400 シリーズ Global Site Selector アプライアンス
- Cisco CatOS

これはすべてを網羅した完全なリストではありません。

詳細

ASN.1 は ITU-T（International Telecommunication Union - Telecommunication Standardization Sector）規格で定義されており、エンコーディング値のデータ構造体などが説明されています。このアドバイザリで説明されている脆弱性は、特定のデータ構造体を解析する実装のみに関連するものであり、規格自体の脆弱性ではありません。

ASN.1 を使用するプロトコル（たとえば、Voice over IP や Simple Network Management Protocol など）であっても、脆弱な暗号ライブラリに依存していない場合は、該当しません。このアドバイザリは、1 つのベンダーから提供される特定の暗号ライブラリにおける実装の問題のみに対処します。

この脆弱性は、次の Cisco 製品に存在します。

- Cisco IOS:Cisco Bug ID CSCsd85587(登録ユーザ専用)に記載されています。
- Cisco IOS XR:Cisco Bug ID CSCsg41084(登録ユーザ専用)に記載されています。
- Cisco PIXおよびASAセキュリティアプライアンス(Cisco Bug ID CSCse91999(登録ユーザ専用))

- Cisco Firewall Services Module(FWSM):Cisco Bug ID CSCsi97695(登録ユーザ専用)に記載されています。
- Cisco Unified CallManager:Cisco Bug ID CSCsg44348(登録ユーザ専用)に記載されています。

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、デバイスの定期的なメンテナンスや操作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。

該当するデバイスに不正なホストがアクセスできないようにすることで、これらの脆弱性が緩和される可能性があります。ネットワーク内部の Cisco のデバイスに展開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 Cisco 適用対応策速報（ https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070522-crypto ）を参照してください。

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は、管理プレーンとコントロールプレーンをターゲットと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 ）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。

```
!-- Include deny statements up front for any protocols/ports/IP addresses that
!-- should not be impacted by CoPP
!-- Include permit statements for the protocols/ports that will be governed by CoPP
!-- port 443 - HTTPS
access-list 100 permit tcp any any eq 443
!-- port 500 - IKE
access-list 100 permit udp any any eq 500
!-- port 848 - GDOI
access-list 100 permit tcp any any eq 848
!-- port 5060 - SIP-TLS
access-list 100 permit tcp any any eq 5060
!-- port 5354 - TIDP
access-list 100 permit tcp any any eq 5354

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.
!
!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.
```

```
!
class-map match-all Drop-Known-Undesirable
 match access-group 100

!
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
!
policy-map CoPP-Input-Policy
 class Drop-Known-Undesirable
  drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.
!
control-plane
 service-policy input CoPP-Input-Policy
```

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が異なることに注意してください。

```
policy-map CoPP-Input-Policy
 class Drop-Known-Undesirable
 police 32000 1500 1500 conform-action drop exceed-action drop
```

注：上記のCoPPの例では、悪用パケットと一致する「permit」アクションを持つACLエントリにより、ポリシーマップのdrop機能によりこれらのパケットが廃棄されますが、「deny」アクションと一致するパケットは、ポリシーマップのdrop機能の影響を受けません。

CoPP 機能の設定と使用に関する詳細は、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd8 および http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html を参照してください。

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

ACL を使用すると、これらの脆弱性を悪用しようとする攻撃を緩和できます。ACL を適用すると、正規の送信元からのパケットのみがデバイスへの到達を許可され、他のパケットはすべてドロップされます。

```
access-list 101 permit tcp host <legitimate_host_IP_address> host <router_IP_address> eq 443
access-list 101 permit udp host <legitimate_host_IP_address> host <router_IP_address> eq 500
access-list 101 permit tcp host <legitimate_host_IP_address> host <router_IP_address> eq 506
access-list 101 permit tcp host <legitimate_host_IP_address> host <router_IP_address> eq 4848
access-list 101 permit tcp host <legitimate_host_IP_address> host <router_IP_address> eq 5060
access-list 101 permit tcp host <legitimate_host_IP_address> host <router_IP_address> eq 5354
access-list 101 deny tcp any any eq 443
```

```
access-list 101 deny udp any any eq 500
access-list 101 deny tcp any any eq 506
access-list 101 deny udp any any eq 4848
access-list 101 deny tcp any any eq 5060
access-list 101 deny tcp any any eq 5354
```

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、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」という用語の詳細については、次のURLを参照してください。http://www.cisco.com/web/about/security/intelligence/ios-ref.html

Cisco IOS

修正済みの Cisco IOS ソフトウェア リリースを次の表に示します。

メジャー リリース	修正済みリリースの入手可能性	
該当する 12.0 ベースのリリース	リビルド	メンテナンス
12.0	12.0 リリースはこの脆弱性に該当しません	

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	12.1 リリースはこの脆弱性に該当しません	
該当する 12.2 ベースのリリース	リビルド	メンテナンス
12.2B	脆弱性あり、12.4(10)以降に移行	
12.2BC	脆弱性：12.3(17b)BC6以降に移行	
12.2BZ	脆弱性あり。TACに連絡	
12.2CX	脆弱性：12.3(17b)BC6以降に移行	
12.2CY	脆弱性：12.3(17b)BC6以降に移行	
12.2CZ	脆弱性あり。TACに連絡	
12.2EWA	12.2(25)EWA9	
12.2EX	脆弱性あり、 12.2(25)SEE3以降に移行	
12.2EY	脆弱性あり、 12.2(25)SEE3以降に移行	

12.2EZ	脆弱性あり、 12.2(25)SEE3以降に移行	
12.2FX	脆弱性あり、 12.2(25)SEE3以降に移行	
12.2FY	脆弱性あり、12.2(35)SE2以降に移行	
12.2FZ	脆弱性あり、12.2(35)SE2以降に移行	
12.2JA	脆弱性あり。TACに連絡	
12.2JK	脆弱性あり、12.4(6)T7以降に移行	
12.2SB	12.2(31)SB2	
12.2SE	12.2(35)SE2	
12.2SEA	脆弱性あり、 12.2(25)SEE3以降に移行	
12.2SEB	脆弱性あり、 12.2(25)SEE3以降に移行	
12.2SEC	脆弱性あり、 12.2(25)SEE3以降に移行	
12.2SED	脆弱性あり、 12.2(25)SEE3以降に移行	

12.2SEE	12.2(25)SEE3	
12.2SEF	脆弱性あり、12.2(35)SE2以降に移行	
12.2SEG	脆弱性あり、12.2(35)SE2以降に移行	
12.2SG		12.2(37)SG
12.2SGA	12.2(31)SGA1	
12.2SRA	12.2(33)SRA3	
12.2SRB		12.2(33)SRB
12.2SXD	脆弱性あり、 12.2(18)SXF8以降に移行	
12.2SXE	脆弱性あり、 12.2(18)SXF8以降に移行	
12.2SXF	12.2(18)SXF8	
12.2T	脆弱性あり、12.3(22)以降に移行	
12.2XR	脆弱性あり、12.3(22)以降に移行	
12.2YU	脆弱性あり、12.4(10)以降に移行	

12.2YV	脆弱性あり、12.4(10)以降に移行	
12.2ZD	脆弱性あり。TACに連絡	
12.2ZE	脆弱性あり、12.3(22)以降に移行	
12.2ZF	脆弱性あり、12.4(10)以降に移行	
12.2ZG	脆弱性あり。TACに連絡	
12.2ZH	脆弱性あり。TACに連絡	
12.2ZJ	脆弱性あり、12.4(10)以降に移行	
12.2ZL	脆弱性あり。TACに連絡	
12.2ZN	脆弱性あり、12.3(22)以降に移行	
12.2ZU	脆弱性あり。TACに連絡	
12.2ZW	脆弱性あり。TACに連絡	
該当する 12.3 ベースのリリース	リビルド	メンテナンス
12.3		12.3(22)

12.3B	脆弱性あり、12.4(10)以降に移行	
12.3BC	12.3(17b)BC6	
	12.3(21a)BC1	
12.3JA	脆弱性あり。TACに連絡	
12.3JEA	脆弱性あり。TACに連絡	
12.3JK	脆弱性あり。TACに連絡	
12.3JL	脆弱性あり。TACに連絡	
12.3JX	脆弱性あり。TACに連絡	
12.3T	脆弱性あり、12.4(10)以降に移行	
12.3TPC	脆弱性あり。TACに連絡	
12.3XA	脆弱性あり。TACに連絡	
12.3XB	脆弱性あり、12.4(10)以降に移行	
12.3XC	脆弱性あり。TACに連絡	
12.3XD	脆弱性あり、12.4(10)以降に移行	

12.3XE	脆弱性あり。TACに連絡	
12.3XF	脆弱性あり、12.4(10)以降に移行	
12.3XG	脆弱性あり。TACに連絡	
12.3XH	脆弱性あり、12.4(10)以降に移行	
12.3XI	脆弱性あり。TACに連絡	
12.3XJ	脆弱性あり。TACに連絡	
12.3XK	脆弱性あり、12.4(10)以降に移行	
12.3XQ	脆弱性あり、12.4(10)以降に移行	
12.3XR	脆弱性あり。TACに連絡	
12.3XS	脆弱性あり、12.4(10)以降に移行	
12.3XU	脆弱性あり、12.4(6)T7以降に移行	
12.3XW	脆弱性あり。TACに連絡	
12.3XX	12.3(8)XX2d	

12.3YA	脆弱性あり。TACに連絡	
12.3YD	脆弱性あり、12.4(6)T7以降に移行	
12.3YF	脆弱性あり。TACに連絡	
12.3YG	脆弱性あり、12.4(6)T7以降に移行	
12.3YH	脆弱性あり、12.4(6)T7以降に移行	
12.3YI	脆弱性あり、12.4(6)T7以降に移行	
12.3YK	脆弱性あり、12.4(6)T7以降に移行	
12.3YQ	脆弱性あり、12.4(6)T7以降に移行	
12.3YS	脆弱性あり、12.4(6)T7以降に移行	
12.3YT	脆弱性あり、12.4(6)T7以降に移行	
12.3YU	脆弱性あり。TACに連絡	
12.3YX	12.3(14)YX7	

12.3YZ	脆弱性あり。TACに連絡	
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(7d)	12.4(10)
12.4SW	12.4(11)SW1	
12.4T	12.4(6)T7	
	12.4(9)T3	
	12.4(11)T1	
12.4XA	脆弱性あり、12.4(6)T7以降に移行	
12.4XB	脆弱性あり。TACに連絡	
12.4XC	12.4(4)XC6	
12.4XD	12.4(4)XD6	
12.4XE	脆弱性あり。TACに連絡	
12.4XJ	12.4(11)XJ2	

Cisco IOS XR

修正済み Cisco IOS XR ソフトウェアの一覧を次の表に示します。

Cisco IOS XR のバージョン	SMU ID	SMU 名
3.2.3	AA01802	hfr-k9sec-3.2.3.CSCsg41084
3.2.4	AA01801	hfr-k9sec-3.2.4.CSCsg41084
3.2.6	AA01800	hfr-k9sec-3.2.6.CSCsg41084
3.3.0	AA01799、AA01780	hfr-k9sec-3.3.0.CSCsg41084
3.3.0	AA01780	c12k-k9sec-3.3.0.CSCsg41084
3.3.1	AA01781	c12k-k9sec-3.3.1.CSCsg41084
3.3.1	AA01798	hfr-k9sec-3.3.1.CSCsg41084
3.3.2	AA01797	hfr-k9sec-3.3.2.CSCsg41084
3.3.3	AA01796	hfr-k9sec-3.3.3.CSCsg41084
3.3.3	AA01785	c12k-k9sec-3.3.3.CSCsg41084

3.4.0	AA01782	c12k-k9sec-3.4.0.CSCsg41084
3.4.0	AA01795	hfr-k9sec-3.4.0.CSCsg41084
3.4.1	AA01783	c12k-k9sec-3.4.1.CSCsg41084
3.4.1	AA01794	hfr-k9sec-3.4.1.CSCsg41084

IOS XR Package Installation Envelopes（PIE）は、https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=IOS-XR（登録ユーザ専用）の File Exchange からダウンロードできます。インストール方法は、付属する .txt ファイルに記載されています。

Cisco PIX および ASA セキュリティ アプライアンス

この脆弱性は、7.0(6.7)、7.1(2.27)、7.2(1.22)、7.2(2) の各 7.x ソフトウェア リリースで修正されています。すべての 8.x ソフトウェア リリースは修正済みのライブラリを使用しており、該当しません。6.x ソフトウェア リリースも、この脆弱性には該当しません。

Cisco Firewall Service Module（FWSM）

この脆弱性は、次のソフトウェア リリースで修正されています。

- 3.1(6) メンテナンス リリース、2007 年 6 月提供予定

Cisco Unified CallManager

この脆弱性は、次のソフトウェア リリースで修正されています。

- 4.0(x) リリースにはこの脆弱性がありますが、修正が提供される予定はありません。修正済みの 4.1 または 4.2 ソフトウェアへのアップグレードを推奨します。
- 4.1(3)sr.5、2007 年 5 月 24 日提供予定
- 4.2(3)sr.2、2007 年 5 月提供予定
- 4.3(1)sr.1、2007 年 6 月提供予定
- 5.0(4) - 修正済みソフトウェアを提供する予定はありません。5.1(2) にアップグレードすることを推奨します
- 5.1(1)：修正済みソフトウェアを提供する予定はありません。5.1(2) にアップグレードする

ことを推奨します
- 5.1(2)

推奨事項

$propertyAndFields.get("recommendations")

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。

この脆弱性は、Cisco の社内テストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto

改訂履歴

リビジョン 1.4	2008年6月27日	概要を更新して、リンクと文言を削除しました。
リビジョン 1.3	2007 年 7 月 28 日	FWSM の 2.3(x) リリースは該当しない
リビジョン 1.2	2007 年 5 月 25 日	修正済み IOS リリースを更新し、IOS の ISAKMP 認証を明記し、IOS XR に対する影響を明記
リビジョン 1.1	2007 年 5 月 22 日	該当する FWSM プロトコルについての情報を更新し、デフォルトで IKE が有効な IOS リリースの種類を修正
リビジョ	2007 年 5 月 22 日	初回公開リリース

ン 1.0		

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。