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 : Yes

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。

これらの脆弱性の何れかの正常な繰り返された利用は支えられたサービス拒否（DoS）の原因となるかもしれません; ただしデータまたはデバイスの機密保持か統合を妥協すると、脆弱性は知られていません。 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 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto で掲示されます。

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。 関連する状況報告は http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL で公開されます

該当製品

修正済みソフトウェア

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。

```
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 ソフトウェア リリースの命名方法に関する詳細については、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。

```
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。

```
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。 デバイスにコマンド `show running` 入力するために設定される HTTPS があったかどうか確認するため `|` 。 HTTPS が有効になっているデバイスの例を次に示します。

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

Threat Information Distribution Protocol（TIDP）

デバイスに有効に なる TDIP があったかどうか確認するためにコマンド `show running-config` 入力して下さい `|  MAP` 。 TDIP が有効になっているデバイスの例を次に示します。

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

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

デバイスに有効に なる SIP-TLS があったかどうか確認するためにコマンド `show running-config` 入力して下さい `|` 。 SIP-TLS が有効になっているデバイスの例を次に示します。

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

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

デバイスに有効に なる EAP-TLS があったかどうか確認するためにコマンド `show running-config` 入力して下さい `|` 。 EAP-TLS が有効になっているデバイスの例を次に示します。

```
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）

デバイスに有効に なる ISAKMP があったかどうか確認するためにコマンド `show running-config` 入力して下さい `| isakmp` 。 IKE が有効になっているデバイスの例を次に示します。

```
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。 デバイスに有効に なる SSL を使用するサービスがあったかどうか確認するために、次のコマンド `show running-config` の 1 つを入力して下さい `| HTTP ssl` か `show running-config | XML CORBA ssl` 。 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。

```
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。 デバイスにコマンド `show running-config` 入力するために有効に なる SSH があったかどうか確認するため `| ssh` 。 SSH が有効になっているデバイスの例を次に示します。

```
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。

```
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。

```
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。

```
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。

```
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。
- **ステップ 2** - 4.x ソフトウェアを実行したら次の作業が必要です: サーバ ドロップダウン リスト ボックスから、パブリッシャー データベース サーバを選択して下さい。 5.x ソフトウェアを実行したら次の作業が必要です: サーバ 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て下さい。
- **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。

改訂履歴

リビジョン 1.4	2008-June-27	リンクおよび冗漫を取除く更新済要約。
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
リビジョン 1.0	2007 年 5 月 22 日	初回公開リリース

利用規約