

# Cisco Security Monitoring, Analysis and Response System(MARS)およびAdaptive Security Device Managerのセキュア通信の脆弱性



アドバイザリーID : Cisco-SA-20070118- [CVE-2007-0397](#)

初公開日 : 2007-01-18 18:11

バージョン 1.0 : Final

CVSSスコア : [4.7](#)

回避策 : No Workarounds available

Cisco バグ ID :

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

バージョン4.2.3より前のCisco Security Monitoring, Analysis and Response System(MARS)およびバージョン5.2(2.1)より前のCisco Adaptive Security Device Manager(ASDM)には、認証されていないリモートの攻撃者がシステムによって管理されるデバイスになりすますことのできる脆弱性が存在します。

この脆弱性は、デバイスが管理対象デバイスからのSSL/TLS証明書またはSSH公開キーを適切に検証していないことに起因します。 認証されていないリモートの攻撃者がこの脆弱性を不正利用して、システムによって管理されているデバイスになりすますことができます。 攻撃者はこれを利用して、認証クレデンシャルなどの機密情報にアクセスしたり、偽のデータをシステムに送信したりする可能性があります。

この脆弱性をエクスプロイトするためにエクスプロイトコードを使用する必要はありません。

シスコはセキュリティアドバイザリーで脆弱性を確認し、更新されたソフトウェアをリリースしました。

影響を受けるアプリケーションは、管理対象デバイスから提示されたSSL/TLS証明書またはSSH公開キーを検証しないため、攻撃者は脆弱なシステムと同じIPアドレスを持つシステムをセ

ットアップし、正当なデバイスではなく偽装デバイスに誤って接続が行われることを期待する可能性があります。これは、IPルーティングの特性を考慮すると、ネットワーク上に同じIPアドレスを持つ複数のシステムが存在する場合に起こります。ただし、このような状況では、ルーティング動作に異常が生じる可能性があります。一部のパケットは正当なシステムに送信される一方で、他のパケットは偽装者に送信される可能性があり、攻撃者が認証クレデンシャルを取得したり、誤解を招く情報を送信したりすることが困難になります。

## 該当製品

シスコは、Cisco Bug ID [CSCsf95930](#)および [CSCsg78595](#)に対処するセキュリティアドバイザリを次のリンクでリリースしました。 [cisco-sa-20070118-certs](#)

### 脆弱性のある製品

次のシスコ製品に脆弱性が存在します。

バージョン4.2.3より前のCisco Security Monitoring, Analysis and Response System(MARS)  
バージョン5.2(2.1)より前のCisco Adaptive Security Device Manager(ASDM)

### 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。

## 回避策

適切なアップデートを適用することを推奨します。

Cisco Adaptive Security Device Manager(ASDM)システムの管理者は、スタンドアロンのASDM Launcherではなく、Webブラウザを使用してASDMサービスを起動することを推奨します。

管理者は、接続が必要なシステムへの接続を制限するために、影響を受けるシステムとその管理対象システムの両方でIPベースのACLを設定することを推奨します。

## 修正済みソフトウェア

契約が有効なシスコのお客様は、Software Center([CS-MARS4.2.3\(2403\)](#))からCisco Security Monitoring, Analysis and Response System(MARS)のアップデートを入手できます。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)に連絡するか、[tac@cisco.com](mailto:tac@cisco.com)のEメールでアップグレードを入手できます。

シスコは、1月22日にAdaptive Security Device Manager(ASDM)のアップデートをリリースする予定です。[ASDM 5.2\(2.1\)](#)

## 推奨事項

\$propertyAndFields.get("recommendations")

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team ( PSIRT ) 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を確認していません。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20070118-CVE-2007-0397>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2007年1月18日

## 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、単独の転載や意識を施した場合、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。