

# Cisco Security Monitoring , Analysis and Response System および Adaptive Security Device Manager セキュアコミュニケーション脆弱性

Medium	アドバイザリーID : Cisco-SA-20070118-CVE-2007-0397	<a href="#">CVE-2007-0397</a>
	初公開日 : 2007-01-18 18:11	<a href="#">バージョン 1.0 : Final</a>
	バージョン 1.0 : Final	
	CVSSスコア : <a href="#">4.7</a>	
	回避策 : <a href="#">Yes</a>	
	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

4.2.3 以前の Cisco Security Monitoring , Analysis and Response System バージョンおよび 5.2(2.1) 以前の Cisco Adaptive Security Device Manager バージョンは非認証を可能にする可能性があるシステムによって管理されるデバイスに扮するために脆弱性がリモート攻撃者含まれています。

管理対象装置からの SSL/TLS 証明書が SSH 公開キーを検証するためにきちんとにのでデバイス存在する脆弱性。A は非認証、リモート攻撃者システムによって管理されたデバイスに扮するのにこの脆弱性を不正利用する可能性があります。A は機密情報への、認証クレデンシャルのようなアクセス権を得るのに攻撃者これを活用する可能性がありますまたはシステムに偽データを入れて下さい。

エクスプロイトコードがこの脆弱性を不正利用するために必要となりません。

Cisco は Security Advisory の脆弱性を確認し、更新済ソフトウェアをリリースしました。

影響を受けたアプリケーションが管理対象装置によって示される SSL/TLS 証明書が SSH 公開キーを検証しないので攻撃者は脆弱なシステムと同じ IP アドレスのシステムを設定し、扮デバイスへの接続が間違っって正当なものよりもむしろなされることを望む可能性があります。しかし同

じ IP アドレス。A のネットワークに複数のシステムがあるときこれが可能性、IP ルーティングの性質が、風変わりなルーティング動作のある A はこのような状態で生じる可能性が高いです。A は困難にする正当なシステムにいくつかのパケット攻撃者が認証を得ることができるように他が役者に送信されるかもしれない間、送信されるかもしれません 資格情報または誤解を招くような情報を送信するため。

## 該当製品

### 修正済みソフトウェア

以下のシスコ製品は脆弱です:

4.2.3 以前の Cisco Security Monitoring , Analysis and Response System バージョン

5.2(2.1) 以前の Cisco Adaptive Security Device Manager バージョン

### 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。

## 改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	<a href="#">初版リリース</a>	該当なし	Final	2007-Jan-18

## 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。