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 **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 :** Yes **Cisco バグ ID :**	CVE-2007-0397

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 証明書か 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。Â 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。Â 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 証明書か 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。Â 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 Â はこのような状態で生じる可能性が高いです。Â 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	初版リリース	該当なし	Final	2007-Jan-18

利用規約