

# Cisco PIXおよびASAのLOCAL方式における特権昇格の脆弱性



アドバイザリーID : Cisco-SA-20070214-[CVE-2007-0960](#)  
初公開日 : 2007-02-14 23:06  
バージョン 1.0 : Final  
CVSSスコア : [6.0](#)  
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

Cisco PIX 500シリーズセキュリティアプライアンスおよびCisco ASA 5500シリーズ適応型セキュリティアプライアンス(ASA)には、認証されたリモートの攻撃者がデバイス上で昇格された特権を取得する可能性のある脆弱性が存在します。

この脆弱性は、ユーザ認証にLOCAL方式を使用するデバイスにのみ存在します。また、攻撃者は、権限0でローカルデータベース内に定義され、デバイスに対して認証できる必要があります。これらの条件が満たされると、攻撃者は自分自身に管理者権限を付与できます。

ベンダーは、この問題に対し、機能的なエクスプロイトコードの可用性を反映したCVSSスコアを提供していますが、このコードが一般に公開されているとは考えられていません。

シスコはこの脆弱性を確認し、更新されたソフトウェアが入手可能であることを確認しました。

この脆弱性をエクスプロイトするには、攻撃者は特権レベル0でローカルデータベースに定義され、影響を受けるデバイスに対して認証できる必要があります。信頼できるユーザだけをローカルデータベースで定義する必要があるため、これらの条件は攻撃の可能性を大幅に減らします。また、影響を受けるデバイスは、デフォルト設定では脆弱ではないことに注意してください。

## 該当製品

シスコは、Cisco Bug ID [CSCsh33287](#)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-20070214-pix](#)

## 脆弱性のある製品

Cisco PIX 500シリーズセキュリティアプライアンスおよびCisco ASA 5500シリーズ適応型セキュリティアプライアンスには、ソフトウェアリリースバージョン7.2.2を使用している場合に脆弱性が存在します。

## 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。

## 回避策

適切なソフトウェアアップデートを適用することを推奨します。

管理者は、ユーザ認証にLOCAL方式を使用する代わりに、認証にTACACS+またはRADIUSのいずれかを使用することを推奨します。Cisco PIXおよびASAアプライアンスでTACACS+またはRADIUSを設定する方法については、次のリンクで確認できます。[PIXおよびASA用のTACACS+およびRADIUSの設定例](#)

LOCAL認証を維持する必要がある管理者は、ユーザの最小権限レベルを0から1に変更することで、この脆弱性を緩和できます。ただし、権限レベル15でない限り、他の適切な権限レベルを使用できます。

管理者は、デバイスへのアクセスを信頼できるユーザのみに制限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、[Cisco](#)のSoftware Centerから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、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、[tac@cisco.com](mailto:tac@cisco.com)に電子メールで問い合わせることでアップグレードを入手できます。

## 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-20070214-CVE-2007-0960>

## 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2月14日

## 利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。