Cisco Secure Access Control Server(ACS)のアカウンティング要求バッファオーバーフローの脆弱性

Medium

アドバイザリーID : Cisco-SA-20070105-CVE-2006-4098　CVE-2006-4098
初公開日 : 2007-01-05 23:00
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 Secure Access Control Server for WindowsおよびCisco Secure Access Control Server(ACS)Solution Engineには、認証されたリモートの攻撃者がサービス妨害(DoS)状態を引き起こしたり、任意のコードを実行したりすることを可能にする脆弱性が存在します。

この脆弱性は、CSRadiusサービスでの不十分な入力検証に起因します。 認証されたリモート攻撃者は、バッファオーバーフローを引き起こすように設計された悪意のあるRADIUSアカウンティング要求を送信することにより、この脆弱性を不正利用する可能性があります。 これにより、攻撃者がこのサービスをクラッシュさせたり、SYSTEM権限で任意のコードを実行したりする可能性があります。

シスコはセキュリティアドバイザリと更新されたソフトウェアをリリースしました。

この脆弱性を不正利用するには、リモート攻撃者がRADIUS秘密キーにアクセスできる必要があります。 これにより、潜在的な攻撃者のプールが減少します。 この不正利用により、攻撃者はCSRadiusサービスの権限で任意のコードを実行する可能性があります。 これは、CSAuthモジュールと、認証および許可サービスを要求するデバイスとの間の通信を提供するために使用されるサービスです。

攻撃者がCSRadiusサービスをクラッシュさせると、すべてのRADIUS認証、許可、アカウンティング(AAA)処理が停止します。 ただし、TACACS+処理は機能し続けます。

該当製品

シスコは、Cisco Bug ID CSCse18278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-20070105-csacs

脆弱性のある製品

次のシスコ製品を実行しているシステムには脆弱性が存在します。

- Cisco Secure Access Control Server(ACS)for Windows 3.1および3.2
- 3.3.4ビルド12より前のCisco Secure Access Control Server for Windows
- 4.0.1ビルド27より前のCisco Secure Access Control Server for Windows
- Cisco Secure Access Control Server(ACS)Solution Engine 3.1および3.2
- 3.3.4ビルド12より前のCisco Secure Access Control Server(ACS)ソリューションエンジン
- 4.0.1ビルド27より前のCisco Secure Access Control Server(ACS)ソリューションエンジン

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。

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。

ACLを実装して、該当システムへのアクセスを制限することが推奨されます。

管理者は、疑わしいアクティビティの兆候がないか該当システムを監視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に電子メールで問い合わせて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-20070105-CVE-2006-4098

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5日

利用規約

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。