Cisco Secure Access Control Server(ACS)のDoS脆弱性

Medium

アドバイザリーID : Cisco-SA-20080903-CVE-2008-2441　CVE-2008-2441
初公開日 : 2008-09-03 17:51
バージョン 1.0 : Final
CVSSスコア : 3.5
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(ACS)には、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、Remote Authentication Dial In User Service(RADIUS)Extensible Authentication Protocol(EAP)応答の処理時のエラーが原因で発生します。 認証されたリモートの攻撃者は、悪意のあるRADIUS EAP応答をターゲットシステムに送信することで、この脆弱性を不正利用する可能性があります。 このアクションにより、認証および認可サービスと、認証を要求するデバイスとの通信に使用されるサービスがクラッシュし、DoS状態が発生する可能性があります。

シスコはこの脆弱性を確認し、更新されたソフトウェアをリリースしました。

攻撃に成功すると、ターゲットシステムの認証サービスが中断される可能性があります。 悪意のあるRADIUS EAP応答を繰り返し送信することで、攻撃者は持続的なDoS状態を引き起こす可能性があります。 この状況では、AAAサーバによる許可に依存するデバイスがネットワークに接続できない可能性があります。

該当製品

シスコは、Cisco Bug ID CSCsq10103に対処するセキュリティ応答を次のリンクでリリースしました：cisco-sr-20080903-csacs

脆弱性のある製品

次のソフトウェアが影響を受けます。

Cisco Secure ACSバージョン3.3.4以前
Cisco Secure ACSバージョン4.0.1以前
Cisco Secure ACSバージョン4.1(4)以前
Cisco Secure ACSバージョン4.2(0)以前

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。

管理者は、可能な限り、影響を受けるシステムへのネットワークアクセスを信頼できるユーザに制限することをお勧めします。

管理者は、RADIUS共有秘密情報を含むアプリケーションの信頼できるシステムへの配布を制限することを推奨します。

管理者は、攻撃を遅延または防止するために、共有秘密情報の変更を検討できます。

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、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のEメール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-20080903-CVE-2008-2441

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	2008年9月3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、単独の転載や意訳を施した場合、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。