Cisco Secure Access Control System TACACS+ Authentication Bypass

Advisory ID: cisco-sa-20121107-acs

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121107-acs

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。

Revision 1.0

For Public Release 2012 November 7 16:00 UTC (GMT)

目次

要約

Cisco Secure Access Control System（ACS）には、認証されていないリモートの攻撃者が、該当製品によって提供される TACACS+ ベースの認証サービスをバイパスできる可能性のある脆弱性が存在します。この脆弱性は、認証プロトコルが TACACS+ となっており、かつ Cisco Secure ACS が外部アイデンティティ ストアの Lightweight Directory Access Protocol（LDAP）を使用した構成になっている場合に、ユーザの入力するパスワードに対する検証が不適切であることに起因します。

攻撃者はユーザ パスワードの入力時に特殊な一連の文字を送信することで、この脆弱性を不正利用できる可能性があります。攻撃者がこの脆弱性を不正利用するには、LDAP 外部アイデンティティ ストアに格納されている有効なユーザ名を知っている必要があり、そのユーザになりすますことによってのみ可能となります。この不正利用によって攻撃者は、TACACS+ と該当する Cisco Secure ACS を使用するあらゆるシステムの認証を通過できる可能性があります。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。この脆弱性に対する回避策はありません。このアドバイザリは、次のリンク先で確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121107-acs

該当製品

脆弱性が存在する製品

次の Cisco Secure ACS バージョンがこの脆弱性の影響を受けます。

Cisco Secure ACS Version	Affected
5.0	Yes
5.1	Yes
5.2	Yes
5.3	Yes
5.4	No

上記は、当該製品のハードウェア アプライアンスおよびソフトウェアのみのバージョンの両方に該当します。

どのバージョンの Cisco Secure ACS がインストールされているかは、次の方法で判別できます。

- Cisco Secure ACS コマンドライン インターフェイス (CLI) で、 **show version** コマンドを実行します。次に例を示します。

```
acs51a/admin# show version

Cisco Application Deployment Engine OS Release: 1.2
ADE-OS Build Version: 1.2.0.152
ADE-OS System Architecture: i386

Copyright (c) 2005-2009 by Cisco Systems, Inc.
All rights reserved.
Hostname: acs51a


Version information of installed applications
---------------------------------------------


Cisco ACS VERSION INFORMATION
-----------------------------
Version : 5.1.0.44.6
Internal Build ID : B.2347
Patches :
5-1-0-44-3
5-1-0-44-6

acs51a/admin#
```

- Cisco Secure ACS の Web ベース インターフェイスのメイン ログイン ページで、画面左側にバージョン情報が表示されます。
- Cisco Secure ACS の Web ベースのインターフェイスからログインして、 画面右上角にある [**About**] リンクをクリックします。

Cisco Secure ACS バージョン 5.1 はバージョン **5.1.0.44** として表示され、Cisco Secure ACS バ

ージョン 5.2 はバージョン **5.2.0.26** として表示され、Cisco Secure ACS バージョン 5.3 はバージョン **5.3.0.40** として表示されます。バージョン番号の後ろに追加された数字は、インストールされている最高のパッチ レベルを表します。たとえば、バージョン番号 **5.1.0.44.3** は、Cisco Secure ACS バージョン 5.1 にパッチ 3 がインストールされていることを示します。バージョン文字列の後ろに数字が追加されていない場合、Cisco Secure ACS バージョンにパッチがインストールされていないことを表します。上の例は、バージョン 5.1 パッチ 6 が実行されている Cisco Secure ACS を示しています。

脆弱性が存在しない製品

次の Cisco Secure ACS 製品はこの脆弱性の影響を受けません。

- Cisco Secure Access Control Server for Windows
- Cisco Secure Access Control Server Express
- Cisco Secure Access Control Server View
- Cisco Secure Access Control Server Solution Engine

他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

詳細

Cisco Secure Access Control System（ACS）は集中管理型の RADIUS および TACACS+ サーバとして動作します。これによって、ユーザ認証、ユーザおよび管理者のデバイス アクセス コントロール、およびポリシー コントロールを、集中管理されたアイデンティティ ネットワーキング ソリューションで実現します。

Cisco Secure ACS は、Cisco Secure ACS ネットワーク リソース リポジトリおよびアイデンティティ ストアを使用して、ネットワーク デバイスおよびその他クライアントに AAA（認証、許可、アカウンティング）サービスを提供します。アイデンティティ ストアは内部または外部のどちらを利用することも可能です。内部アイデンティティ ストアは、ユーザ クレデンシャル情報を内部のデータベースに格納しています。外部アイデンティティ ストアでは、Cisco Secure ACS が外部データベースから情報を取得します。

Cisco Secure Access Control System（ACS）には、認証されていないリモートの攻撃者が、該当製品によって提供される TACACS+ ベースの認証サービスをバイパスできる可能性のある脆弱性が存在します。

この脆弱性は、認証プロトコルが TACACS+ となっており、かつ Cisco Secure ACS が外部アイデンティティ ストアの Lightweight Directory Access Protocol（LDAP）を使用した構成になっている場合に、ユーザの入力するパスワードに対する検証が不適切であることに起因します。
攻撃者はユーザ パスワードの入力時に特殊な一連の文字を送信することで、この脆弱性を不正利用できる可能性があります。攻撃者がこの脆弱性を不正利用するには、LDAP 外部アイデンティティ ストアに格納されている有効なユーザ名を知っている必要があり、そのユーザになりすますことによってのみ可能となります。この不正利用によって攻撃者は、TACACS+ と該当する Cisco Secure ACS を使用するあらゆるシステムの認証を通過できる可能性があります。

注：この脆弱性は、TACACS+ 認証が設定されており、かつ LDAP を外部アイデンティティ ストアとして使用する Cisco Secure ACS のみに存在します。
サポートされている他のプロトコル（RADIUS など）と組み合わせて、または TACACS+ が内部アイデンティティ ストアまたは該当しない外部ストア（たとえば RADIUS Identity Server、Active Directory、RSA SecurID Token Server など）と組み合わせて認証サービスに使用されている場合、その Cisco Secure ACS には この脆弱性は存在しません。

攻撃者がこの脆弱性の不正利用に成功した場合、TACACS+ を使用し、かつ脆弱性の影響を受ける Cisco Secure ACS が提供する認証サービスを利用しているシステムすべての認証をバイパスする可能性があります。ただし、攻撃者が Cisco Secure ACS の管理インターフェイスに不正アクセスすることはできません。

この脆弱性は、Cisco Bug ID CSCuc65634（ 登録ユーザ専用 ）として文書化され、 CVE ID として CVE-2012-5424 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

Cisco Secure ACS TACACS+ Authentication Bypass Vulnerability - CSCuc65634 Calculate the environmental score of					
CVSS Base Score - **5.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	None	None
CVSS Temporal Score - **4.1**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、リモートの攻撃者はユーザを装うことで、TACACS+ を使用し、かつ脆弱性の影響を受ける Cisco Secure ACS が提供する認証サービスを利用しているシステムすべての認証をバイパスする可能性があります。

ソフトウェア バージョンおよび修正

次の表に、このセキュリティ アドバイザリに記載した脆弱性を緩和するためのソフトウェア アップグレードの情報を示します。

Cisco Secure ACS Version	Fixed Release
5.0	Migrate to 5.2 Patch 11
5.1	Migrate to 5.2 Patch 11
5.2	5.2 Patch 11
5.3	5.3 Patch 7

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories and Responses アーカイブや、本アドバイザリ以降に公開のアドバイザリを参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明確な場合は、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

回避策

この脆弱性に対する回避策はありません。この脆弱性の不正利用を防ぐために、可能であれば LDAP 外部アイデンティティ ストアの匿名バインディングを無効にするか、または Active Directory 外部アイデンティティ ストアを使用してください。

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレードを入手することができます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、適切な処置について支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策または修正が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC を通して無償アップグレードをお求めください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、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とその公表は確認しておりません。

この脆弱性はサポート ケースの解決中に発見されたものです。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121107-acs

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

このアドバイザリに関する今後の更新があれば、Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-November-07	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。