Cisco Secure Access Control System TACACS+認証バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-20121107-acs CVE-2012-5424
初公開日 : 2012-11-07 16:00
バージョン 1.0 : Final
CVSSスコア : 5.0
回避策 : No Workarounds available
Cisco バグ ID : CSCuc65634

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 System(ACS)には脆弱性があり、認証されていないリモートの攻撃者が該当製品が提供するTACACS+ベースの認証サービスをバイパスできる可能性があります。この脆弱性は、TACACS+が認証プロトコルであり、Cisco Secure ACSがLightweight Directory Access Protocol(LDAP)外部アイデンティティストアで設定されている場合に、ユーザが指定するパスワードの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を求められたときに特殊な文字シーケンスを送信することで、この脆弱性を不正利用する可能性があります。攻撃者がこの脆弱性を不正利用するには、LDAP外部IDストアに保存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が制限されます。この不正利用により、攻撃者はTACACS+を該当のCisco Secure ACSと組み合わせて使用している任意のシステムへの認証に成功する可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121107-acs

該当製品

脆弱性のある製品

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

Cisco Secure ACSのバージョン	該当
5.0	Yes

5.1	Yes
5.2	Yes
5.3	Yes
5.4	いいえ

上記のリストは、ハードウェアアプライアンスとソフトウェアのみのバージョンの両方に適用されます。

インストールされているCisco Secure ACSのバージョンは、次の方法で確認できます。

- Cisco Secure ACSのコマンドラインインターフェイス(CLI)から、次の例に示すようにshow versionコマンドを発行します。

```
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、バージョン情報が画面の左側に表示されます。
- Cisco Secure ACSのWebベースインターフェイスからログインして、画面の右上隅にある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、Cisco Secure ACSバージョン5.2はバージョン5.2.0.26、Cisco Secure ACSバージョン5.3はバージョン5.3.0.40として識別されます。バージョン番号の後に追加の数字が表示されている場合は、インストールされている最高のパッチレベルを示します。たとえば、バージョン番号5.1.0.44.3は、パッチ3がインストールさ

れているCisco Secure ACSバージョン5.1を示します。バージョン文字列の後に追加の数字が表示されない場合は、パッチがインストールされていないCisco Secure ACSのバージョンを示しています。上記の例は、バージョン5.1パッチ6を実行しているCisco Secure ACSを示しています。

脆弱性を含んでいないことが確認された製品

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。

詳細

Cisco Secure Access Control System(ACS)は、一元化されたRADIUSおよびTACACS+サーバとして動作し、ユーザ認証、ユーザおよび管理者のデバイスアクセス制御、ポリシー制御を1つの一元化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に統合します。

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のクライアントに認証、許可、アカウンティング(AAA)サービスを提供します。ID ストアは内部でも外部でも可能です。内部アイデンティティストアは、内部データベースに保存されたユーザクレデンシャル情報を持ちます。外部アイデンティティストアでは、Cisco Secure ACSは外部データベースから情報を取得します。

Cisco Secure Access Control System(ACS)には脆弱性があり、認証されていないリモートの攻撃者が該当製品が提供するTACACS+ベースの認証サービスをバイパスできる可能性があります。

この脆弱性は、TACACS+が認証プロトコルであり、Cisco Secure ACSがLightweight Directory Access Protocol(LDAP)外部アイデンティティストアで設定されている場合に、ユーザが指定するパスワードの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を求められたときに特殊な文字シーケンスを送信することで、この脆弱性を不正利用する可能性があります。攻撃者がこの脆弱性を不正利用するには、LDAP外部IDストアに保存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が制限されます。この不正利用により、攻撃者はTACACS+を該当のCisco Secure ACSと組み合わせて使用している任意のシステムへの認証に成功する可能性があります。

注：脆弱性が存在するのは、TACACS+認証用に設定され、外部IDストアとしてLDAPを使用するCisco Secure ACSだけです。
認証サービスに他のサポートされているプロトコル（RADIUSなど）を組み合わせて使用する

Cisco Secure ACS、または内部IDストアやその他の外部ストア（RADIUS Identity Server、Active Directory、RSA SecurID Token Serverなど）と組み合わせて使用するTACACS+ は脆弱ではありません。

この脆弱性の不正利用に成功すると、攻撃者はTACACS+を使用し、該当するCisco Secure ACSによって提供される認証サービスに依存するシステムの認証をバイパスできる可能性があります。ただし、攻撃者はCisco Secure ACSの管理インターフェイスへの不正アクセスを取得できません。

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。

回避策

この脆弱性に対する回避策はありません。可能であれば、LDAP外部IDストアで匿名バインディングを無効にするか、Active Directory外部IDストアを使用してこの脆弱性の不正利用を防止してください。

修正済みソフトウェア

次の表に、このセキュリティアドバイザリに記載され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情報を示します。

Cisco Secure ACSのバージョン	修正済みリリース
5.0	5.2 パッチ 11 への移行が必要
5.1	5.2 パッチ 11 への移行が必要
5.2	5.2 パッチ 11
5.3	5.3 パッチ 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 アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、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。

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。

この脆弱性は、サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121107-acs

改訂履歴

リビジョン 1.0	2012年11月7日	初回公開リリース

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。