Cisco Unified Communications Manager IP Phone Personal Address Book Synchronizerの権限昇格の脆弱性

アドバイザリーID : cisco-sa-20090311-cucmpab
初公開日 : 2009-03-11 16:00
バージョン 1.0 : Final
CVSSスコア : 9.0
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2009-0632

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 Unified Communications Manager（旧称CallManager）のIP Phone Personal Address Book(PAB)Synchronizer機能に権限昇格の脆弱性が存在します。この脆弱性により、攻撃者は脆弱性のあるCisco Unified Communications Managerシステムに対する完全な管理アクセス権を取得できる場合があります。Cisco Unified Communications Managerが外部ディレクトリサービスと統合されている場合、攻撃者が権限昇格の脆弱性を利用して、認証にディレクトリサービスを使用するように設定された追加のシステムにアクセス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。この脆弱性に対しては回避策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090311-cucmpab で公開されています。

該当製品

脆弱性のある製品

次の製品に脆弱性が存在します。

- Cisco Unified CallManager 4.1バージョン
- 4.2(3)SR4bよりも前のCisco Unified Communications Manager 4.2バージョン
- 4.3(2)SR1bよりも前のCisco Unified Communications Manager 4.3バージョン

- 5.1(3e)より前のCisco Unified Communications Manager 5.xバージョン
- 6.1(3)よりも前のCisco Unified Communications Manager 6.xバージョン
- 7.0(2)よりも前のCisco Unified Communications Manager 7.0バージョン

Cisco Unified Communications Managerソフトウェアバージョン4.xを実行しているシステムの管理者は、Cisco Unified Communications Manager管理インターフェイスでHelp > About Cisco Unified CallManagerの順に選択し、Detailsボタンを選択することで、ソフトウェアバージョンを確認できます。

Cisco Unified Communications Managerソフトウェアバージョン5.x、6.x、および7.xを実行しているシステムの管理者は、Cisco Unified Communications Manager管理インターフェイスのメインページを表示してソフトウェアバージョンを確認できます。ソフトウェアのバージョンは、Command Line Interface（CLI; コマンド ライン インターフェイス）で show version active コマンドを実行して確認することもできます。

脆弱性を含んでいないことが確認された製品

Cisco Unified Communications Manager Expressは、この脆弱性の影響を受けません。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 Unified Communications ManagerのCisco IP Phone Personal Address Book(PAB)Synchronizer機能を使用すると、Cisco Unified Communications Managerのアドレス帳をMicrosoft Windowsのアドレス帳と同期させることができます。IP Phone PAB Synchronizer機能には、権限昇格の脆弱性が含まれており、攻撃者が脆弱性のあるCisco Unified Communications Managerシステムへの完全な管理アクセス権を取得できる可能性があります。IP Phone PAB Synchronizerクライアントが、HTTPS接続を介してCisco Unified Communications Managerデバイスに対する認証に成功すると、Cisco Unified Communications Managerは、Cisco Unified Communications Managerディレクトリサービスの管理に使用するユーザアカウントのクレデンシャルを返します。攻撃者がクレデンシャルを傍受できる場合、Cisco Unified Communications Managerの設定に不正な変更を加え、権限を拡張できます。IP Phone PAB Synchronizerクライアントは、ディレクトリサービスのクレデンシャルを必要とせずにアドレス帳を同期できるように再設計されています。この脆弱性を悪用しても、攻撃者はCisco Unified Communications Managerシステムの基盤となるプラットフォームのオペレーティングシステムにアクセスすることはできません。

Cisco Unified Communications Manager 4.x

Cisco Unified Communications Managerソフトウェアバージョン4.xは、デフォルトで、DC Directoryと呼ばれる内部Lightweight Directory Access Protocol(LDAP)サーバを使用してユーザ情報を保存します。IP Phone PAB Synchronizerクライアントが正常に認証されると、Cisco Unified Communications ManagerはDC Directoryユーザのクレデンシャルを返します。このクレデンシャ

ルは、クライアントがユーザのアドレス帳を同期するために使用されます。Cisco Unified Communications Managerの設定方法によっては、攻撃者が代行受信したクレデンシャルを使用して異なる特権レベルを取得する可能性があります。

デフォルトでは、Cisco Unified Communications Managerソフトウェアバージョン4.xの管理者アカウントは、基盤となるMicrosoft Windowsオペレーティングシステムの一部として作成されます。Cisco Unified Communications Managerは、エンタープライズ環境へのCisco Unified Communications Managerの統合を容易にするために、一般にマルチレベル管理(MLA)機能を使用して導入されます。MLAが有効な場合、Cisco Unified Communications ManagerはCisco Unified Communications Manager DC Directoryサービスに管理者アカウントを保存します。攻撃者がDC Directoryクレデンシャルを取得し、MLAが有効になっている場合、攻撃者は既存のアカウントをCisco Unified Communications Managerスーパーユーザグループに追加できます。攻撃者は、完全な管理アクセス権を持つCisco Unified Communications Manager管理インターフェイスにアクセスできます。MLAが有効でない場合、攻撃者は特権を昇格できませんが、ディレクトリ内のユーザ設定を変更することはできます。

Cisco Unified Communications Manager 4.x IP Phone PAB Synchronizerクライアントは、暗号化されていないLDAP接続を使用してアドレス帳を同期します。DC Directoryのクレデンシャルはネットワーク上でクリアテキストで渡され、攻撃者によってスニッフィングされる危険性があります。DC Directory内部LDAPサーバを使用している場合、IP Phone PAB Synchronizerクライアントは TCPポート8404および8405でCisco Unified Communications Managerと通信します。

Cisco Unified Communications Manager 5.x、6.x、7.x

Cisco Unified Communications Managerソフトウェアバージョン5.x、6.x、および7.xは、ユーザ情報を内部Cisco Unified Communications Manager設定データベースの一部として保存します。IP Phone PAB Synchronizerクライアントは、AXLアプリケーションプログラミングインターフェイス(API)を使用してアドレス帳の同期を実行します。クライアントが正常に認証されると、Cisco Unified Communications Managerは、TabSyncSysUserという名前のデータベースユーザアカウントのクレデンシャルを返します。このアカウントは、クライアントがユーザのアドレス帳を同期するために使用されます。TabSyncSysUserアカウントには、Cisco Unified Communications Manager設定データベースに対する完全な読み取りおよび書き込み権限があります。攻撃者は、AXL API経由でTabSyncSysUserクレデンシャルを使用して、新しい管理者アカウントの作成など、データベース内の任意のパラメータを変更できます。

ディレクトリサービスの統合

Cisco Unified Communications Managerソフトウェアバージョン4.x、5.x、6.x、および7.xは、Microsoft Active Directoryおよび複数の非Microsoft LDAPサーバと統合して、ユーザ認証を実行できます。統合プロセスが正しく機能するには、ディレクトリサービスの適切なユーザクレデンシャルがCisco Unified Communications Managerに提供されている必要があります。攻撃者がIP Phone PAB Synchronizerクライアントに応答するCisco Unified Communications Managerから返されたディレクトリサービスのクレデンシャルを傍受または傍受すると、攻撃者はそのクレデン

シャルを利用して、認証にディレクトリサービスを使用するように設定された追加のシステムにアクセスできる可能性があります。

管理者は、Cisco Unified Communications Manager統合プロセスに使用されるすべてのディレクトリサービスのクレデンシャルが、最小権限の原則に従うように設定されていることを確認する必要があります。クレデンシャルは、統合プロセスが正しく機能するために必要なディレクトリサービスデータにアクセスするために必要な特権だけを設定する必要があります。過度に特権のある管理者アカウントの使用は推奨されません。最小権限の概念を使用してCisco Unified Communications ManagerとADの統合を実行する方法の詳細については、「回避策」セクションを参照してください。

この脆弱性は、Cisco Bug ID CSCso76587およびCSCso78528（登録ユーザ専用）として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-0632が割り当てられています。

回避策

次の回避策を使用して、この脆弱性を緩和できます。

Cisco Unified Communications Manager 4.x

この脆弱性は、IP Phone Personal Address Book(PAB)のScynchronizerクライアントが対話するASPスクリプトを、Cisco Unified Communications Manager Webサーバからアクセスできないディレクトリの場所に移動することで軽減できます。ASPスクリプトが格納されるシステムドライブは、Cisco Unified Communications Managerのインストール方法によって異なります。この回避策を使用すると、アドレス帳の同期が防止されますが、PABアプリケーションは引き続き機能します。ASPスクリプトは、次のコマンドを使用して移動できます。

```
C:\> move c:\CiscoWebs\User\LDAPDetails.asp c:\temp
```

また、スクリーニングデバイスにフィルタリングを実装するか、Windowsファイアウォールを使用して、この脆弱性を緩和することもできます。管理者は、信頼できるネットワークからのみTCPポート8404および8405へのアクセスを許可することを推奨します。

Cisco Unified Communications Manager 5.x、6.x、7.x

この脆弱性は、TabSyncSysUserデータベースユーザアカウントの権限を制限することで緩和できます。Cisco Unified Communications Manager Administrationインターフェイスで、User Management > Application Userの順に移動し、TabSyncSysUserアカウントを検索します。アカウントからすべてのグループを削除し、パスワードを変更します。この回避策を使用すると、アドレス帳の同期が防止されますが、PABアプリケーションは引き続き機能します。

Active Directoryの統合

Cisco Unified Communications ManagerとActive Directory(AD)の統合のセキュリティを向上させるために、シスコは、最小権限の原則を使用してCisco Unified Communications ManagerとADの統合を実行する方法の詳細な説明を記載したホワイトペーパーを作成しました。ホワイトペーパーは次のサイトからダウンロードできます。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a0080a83435.shtml

ネットワーク内のCiscoデバイスに展開できる追加の緩和テクニックについては、このアドバイザリに関連するCisco適用対応策速報を参照してください。

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090311-cucmpab

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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機器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。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco Unified Communications Managerソフトウェアバージョン4.2(3)SR4bには、この脆弱性に対する修正が含まれています。Cisco Unified CallManagerソフトウェアバージョン4.1システムの管理者は、修正済みソフトウェアを入手するために、Cisco Unified Communications Managerソフトウェアバージョン4.2(3)SR4bにアップグレードすることをお勧めします。バージョン4.2(3)SR4bは、次のリンクからダウンロードできます。

https://sec.cloudapps.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communicatio

Cisco Unified Communications Managerソフトウェアバージョン4.3(2)SR1bには、この脆弱性に対する修正が含まれています。バージョン4.3(2)SR1bは、次のリンクからダウンロードできます。

https://sec.cloudapps.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communicatio

Cisco Unified Communications Managerソフトウェアバージョン5.1(3e)には、この脆弱性に対する修正が含まれています。バージョン5.1(3e)は、次のリンク先からダウンロードできます。

https://sec.cloudapps.cisco.com/support/downloads/go/ReleaseType.x?optPlat=null&isPlatform=Y&mdfid=

Cisco Unified Communications Managerソフトウェアバージョン6.1(3)には、この脆弱性に対する

修正が含まれています。バージョン6.1(3)は、次のリンク先からダウンロードできます。

https://sec.cloudapps.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communicatio

Cisco Unified Communications Managerソフトウェアバージョン7.0(2)には、この脆弱性に対する修正が含まれています。バージョン7.0(2)は、次のリンクからダウンロードできます。

https://sec.cloudapps.cisco.com/support/downloads/go/ReleaseType.x?optPlat=&isPlatform=Y&mdfid=28

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco 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やその公表は確認しておりません。

Cisco Unified Communications Manager 4.xソフトウェアバージョンの脆弱性は、Dimension Data FranceのOlivier Grosjeanne氏によってシスコに報告されました。Cisco Unified Communications Manager 5.x、6.x、および7.xソフトウェアバージョンの脆弱性は、LBIのOliver Dewdney氏によって報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090311-cucmpab

改訂履歴

リビジョン 1.0	2009年3月11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。