Cisco Unified Communications Managerのスタティック SSHクレデンシャルの脆弱性

アドバイザリーID : cisco-sa-cucm-ssh-m4UBdpE7
初公開日 : 2025-07-02 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCwp27755

CVE-2025-20309

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(Unified CM)およびCisco Unified Communications Manager Session Management Edition(Unified CM SME)の脆弱性により、認証されていないリモートの攻撃者が、デフォルトの静的クレデンシャル（変更や削除ができない）であるrootアカウントを使用して該当デバイスにログインする可能性があります。

この脆弱性は、開発時に使用するために予約されているrootアカウントの静的なユーザクレデンシャルが存在することに起因します。攻撃者は、そのアカウントを使用して該当システムにログインすることで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は root ユーザで影響を受けるシステムにログインし、任意のコマンドの実行が可能になります。

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。この脆弱性に対処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-cucm-ssh-m4UBdpE7

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、Cisco Unified CMおよびUnified CM SME Engineering Special(ES)リリース15.0.1.13010-1 ~ 15.0.1.13017-1に影響を与えます。

注：ESリリースは、Cisco Technical Assistance Center(TAC)のみが配布する制限付き修正リリースです。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

セキュリティ侵害の痕跡

『Cisco Security Indicators of Compromise Reference Guide』にはよく見られる IoC が記載されており、このシスコ セキュリティ アドバイザリで公開されている脆弱性の影響を受ける可能性のあるデバイスを特定するのに役立ちます。

不正利用に成功すると、rootユーザに対して/var/log/active/syslog/secureへのログエントリがroot権限で作成される可能性があります。このイベントのロギングはデフォルトで有効になっています。

ログを取得するには、CLIから次のコマンドを実行します。

```
cucm1# file get activelog syslog/secure
```

ログエントリに両方ともsshdが含まれており、ユーザrootによるSSHログインの成功が示されている場合、それは次の例に示すようにIoCです。

<#root>

```
Apr 6 10:38:43 cucm1 authpriv 6 systemd: pam_unix(systemd-user:session): session opened for user root by
Apr 6 10:38:43 cucm1 authpriv 6
```

sshd

```
: pam_unix(sshd:session): session opened for user
```

root

```
 by (uid=0)
```

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

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リリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ 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、お客様は以下のリンクに記載された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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、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。

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 TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco Unified CM および Unified CM SME のリリース	First Fixed Release（修正された最初のリリース）
12.5	脆弱性なし
14	脆弱性なし
15.0.1.13010-1 ～ 15.0.1.13017-11	15SU3（2025年7月）またはapply patch file: ciscocm.CSCwp27755_D0247-1.cop.sha512

1. 脆弱性が存在するのは、上記の一連のESリリースだけです。どのリリースのサービスアップデート(SU)も影響を受けません。

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

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。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssh-m4UBdpE7

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	初回公開リリース	—	Final	2025年7月2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。