クラウドプラットフォーム上の Cisco Identity Services Engine の静的ログイン情報の脆弱性

Critical

アドバイザリーID : cisco-sa-ise-aws-static-cred-FPMjUcm7
CVE-2025-20286
初公開日 : 2025-06-04 16:00
最終更新日 : 2025-06-05 17:26
バージョン 1.3 : Final
CVSSスコア : 9.9
回避策 : No workarounds available
Cisco バグ ID : CSCwn63400

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 Identity Services Engine（ISE）の Amazon Web Services（AWS）、Microsoft Azure、および Oracle Cloud Infrastructure（OCI）のクラウド展開における脆弱性により、認証されていないリモートの攻撃者が、機密データへのアクセス、制限された管理操作の実行、システム設定の変更、または影響を受けるシステム内のサービスの中断を引き起こす可能性があります。

この脆弱性は、Cisco ISE がクラウドプラットフォームに展開されているときにログイン情報が不適切に生成され、同じログイン情報が異なる Cisco ISE 展開で共有されることに起因します。これらのログイン情報が複数の Cisco ISE 展開の間で共有されるのは、ソフトウェアリリースとクラウドプラットフォームが同じである場合に限ります。攻撃者は、クラウドに展開されている Cisco ISE からユーザーログイン情報を抽出し、それを使用して、セキュリティで保護されていないポートを介して他のクラウド環境に展開されている Cisco ISE にアクセスすることで、この脆弱性をエクスプロイト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、機密データへのアクセス、制限された管理操作の実行、システム設定の変更、または影響を受けるシステム内のサービスの中断を引き起こす可能性があります。

注：プライマリ管理ノードがクラウドに展開されている場合、Cisco ISE はこの脆弱性の影響を受けます。プライマリ管理ノードがオンプレミスの場合は、影響を受けません。

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-ise-aws-

static-cred-FPMjUcm7

該当製品

脆弱性のある製品

この脆弱性は、AWS、Azure、および OCI の各プラットフォームに展開されている場合に、デフォルト設定の以下の Cisco ISE リリースに影響します。

Platform	Cisco ISE の脆弱性のあるリリース
AWS	3.1、3.2、3.3、および 3.4
Azure	3.2、3.3、および 3.4
OCI	3.2、3.3、および 3.4

注：プライマリ管理ノードがクラウドに展開されている場合、Cisco ISE はこの脆弱性の影響を受けます。プライマリ管理ノードがオンプレミスの場合は、影響を受けません。

修正済みのシスコ プラットフォーム リリースの詳細については、このアドバイザリの「修正済みソフトウェア」の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。

この脆弱性は、Cisco ISE の以下の展開には影響しません。

- アーティファクトが Cisco Software Download Center（ISO または OVA）からインストールされているフォームファクタでのすべてのオンプレミスへの導入。 これには、さまざまなフォームファクタのアプライアンスと仮想マシンが含まれます。
- Azure VMware ソリューション（AVS）上の ISE
- Google Cloud VMware Engine 上の ISE
- AWS での VMware Cloud 上の ISE
- すべての ISE 管理者ペルソナ（プライマリおよびセカンダリ管理）をオンプレミスに、その他のペルソナをクラウドに配置した ISE ハイブリッド展開。

詳細

クラウドに展開される Cisco ISE に存在するログイン情報は、各リリースとプラットフォームに固有です。例：

- AWS 上の リリース 3.1 のすべてのインスタンスには、同じ静的ログイン情報が設定されています。

- リリース 3.1 展開へのアクセスに有効なログイン情報は、同じプラットフォーム上のリリース 3.2 展開へのアクセスには有効ではありません。
- AWS のリリース 3.2 には、Azure のリリース 3.2 と同じログイン情報はありません。

回避策

この脆弱性に対処する回避策はありません。ただし、次のような緩和策があります。

- クラウド セキュリティ グループを使用する送信元 IP を許可する：クラウドプラットフォームでセキュリティグループを使用する顧客管理者の送信元 IP アドレスを許可すると、トラフィックが Cisco ISE インスタンスに到達する前に、承認された管理者のみにアクセスを制限し、悪意のある可能性がある接続を効果的にブロックします。
- Cisco ISE で送信元 IP を許可する：Cisco ISE UI で、顧客管理者の送信元 IP アドレスを許可します。

新規インストールの場合、application reset-config ise コマンドを実行して、ユーザーパスワードを新しい値にリセットします。application reset-config ise コマンドの実行は、クラウド内のプライマリ管理ペルソナノードでのみ必要です。セカンダリノードをリセットする必要はありません。プライマリ管理ペルソナがオンプレミスの場合、コマンドを実行する必要はありません。

警告：

- application reset-config ise コマンドを実行すると、Cisco ISE が工場出荷時の設定にリセットされます。詳細については、『Cisco ISE コンフィギュレーション ガイド』を参照してください。
- 復元されている構成バックアップが脆弱性の修正が適用される前に取得されたものである場合、古いログイン情報も復元されます。修正のインストール後に新しい構成バックアップを作成して、古いログイン情報が復元されないようにすることを推奨します。古いバックアップが復元されている場合は、ホットフィックスを削除して再インストールする必要があります。

これらの緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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。中央の列にはそのリリースに利用可能なホットフィックスが示され、右側の列には脆弱性に対して最初に修正されたリリースが示されます。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 ISE リリース	ホットフィックス	First Fixed Release（修正された最初のリリース）
3.0 以前	該当なし	影響なし。
3.1	ise-apply-CSCwn63400_3.1.x_patchall-SPA.tar.gz このホットフィックスは、リリース 3.1 ～ 3.4 に適用されます。	修正済みリリースに移行。
3.2	ise-apply-CSCwn63400_3.1.x_patchall-SPA.tar.gz このホットフィックスは、リリース 3.1 ～ 3.4 に適用されます。	修正済みリリースに移行。
3.3	ise-apply-CSCwn63400_3.1.x_patchall-SPA.tar.gz このホットフィックスは、リリース 3.1 ～ 3.4 に適用されます。	3.3P8（2025 年 11 月）
3.4	ise-apply-CSCwn63400_3.1.x_patchall-SPA.tar.gz このホットフィックスは、リリース 3.1 ～ 3.4 に適用されます。	3.4P3（2025 年 10 月）
3.5	該当なし	リリース予定（2025 年 8 月）

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 は、このアドバイザリで説明されている脆弱性に対してコンセプト実証エクスプロイトコードが利用可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

シスコは、この脆弱性を報告していただいた GMO Cybersecurity by Ierae 社の Kentaro Kawane 氏に謝意を表します。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-

static-cred-FPMjUcm7

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.3	構成バックアップに関する警告を追加。	回避策	Final	2025 年 6 月 5 日
1.2	影響を受けないリリース 3.0 を追加。	修正済みリリース	Final	2025 年 6 月 5 日
1.1	将来の修正情報を追加。	修正済みリリース	Final	2025 年 6 月 4 日
1.0	初回公開リリース	—	Final	2025 年 6 月 4 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。