Cisco Identity Services Engine の認証されていないリモートコード実行の脆弱性

アドバイザリーID : cisco-sa-ise-unauth-rce-ZAd2GnJ6
初公開日 : 2025-06-25 16:00
最終更新日 : 2025-07-24 23:30
バージョン 2.2 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCwo99449 CSCwp02814 CSCwp02821

CVE-2025-20337
CVE-2025-20281
CVE-2025-20282

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）および Cisco ISE Passive Identity Connector（ISE-PIC）にある複数の脆弱性により、認証されていないリモートの攻撃者が、基盤となるオペレーティングシステムでルートユーザーとしてコマンドを発行する可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これらの脆弱性に対処する回避策はありません。

注：このアドバイザリのバージョン1.0の公開以降、改善された修正済みリリースが利用可能になりました。シスコでは、次のように修正済み拡張リリースにアップグレードすることを推奨しています。

- Cisco ISEがリリース3.4パッチ2を実行している場合、これ以上の操作は必要ありません。
- Cisco ISEがリリース3.3パッチ6を実行している場合、リリース3.3パッチ7で追加の修正が利用可能であり、デバイスをアップグレードする必要があります。
- Cisco ISEにホットパッチ ise-apply-CSCwo99449_3.3.0.430_patch4-SPA.tar.gzまたはホットパッチise-apply-CSCwo99449_3.4.0.608_patch1-SPA.tar.gzがインストールされている場合、リリース3.3パッチ7またはリリース3.4パッチ2にアップグレードすることをお勧めします。このホットパッチはCVE-2025-20337に対応していないため、CCOから保留されています。

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-unauth-rce-ZAd2GnJ6

該当製品

脆弱性のある製品

CVE-2025-20281 および CVE-2025-20337：これらの脆弱性は、デバイスの設定に関係なく、Cisco ISE および ISE-PIC リリース 3.3 と 3.4 に影響を与えます。この脆弱性は、Cisco ISE および ISE-PIC リリース 3.2 以前には影響しません。

CVE-2025-20282：この脆弱性は、デバイスの設定に関係なく、Cisco ISE および ISE-PIC リリース 3.4 にのみ影響します。この脆弱性は、Cisco ISE および ISE-PIC リリース 3.3 以前には影響しません。

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」セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2025-20281 および CVE-2025-20337：Cisco ISE API における認証されていないリモートコード実行の脆弱性

Cisco ISE および Cisco ISE-PIC の特定の API における複数の脆弱性により、認証されていないリモートの攻撃者が、基盤となるオペレーティングシステムで root として任意のコードを実行する可能性があります。攻撃者がこれらの脆弱性をエクスプロイトするのに、有効なクレデンシャルは必要ありません。

この脆弱性は、ユーザ提供による入力の検証が不十分であることが原因です。攻撃者は、巧妙に細工された API 要求を送信することで、これら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、攻撃者は該当デバイスでルート権限を取得する可能性があります。

シスコはこれら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。これらの脆弱性に対処する回避策はありません。

バグ ID：CSCwo99449 および CSCwp02814

CVE ID：CVE-2025-20281、CVE-2025-20337
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：10.0
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE-2025-20282：Cisco ISE API の認証されていないリモートコード実行の脆弱性

Cisco ISE および Cisco ISE-PIC の内部 API 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、該当デバイスに任意のファイルをアップロードし、基盤となるオペレーティングシステムでルートとしてそのファイルを実行する可能性があります。

この脆弱性は、アップロードされたファイルが該当システムの特権ディレクトリに配置されないようにするファイル検証チェックが不十分であることに起因します。攻撃者は、巧妙に細工されたファイルを該当デバイスにアップロードすることにより、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、攻撃者は該当システムに悪意のあるファイルを保存し、任意のコードを実行したり、システムでルート権限を取得したり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。この脆弱性に対処する回避策はありません。

バグ ID：CSCwp02821
CVE ID：CVE-2025-20282
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：10.0
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

回避策

これら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

次の表に示すように、該当する修正済みの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。

注：このアドバイザリのバージョン 1.0 の公開以降、改善された修正済みリリースが利用可能になりました。シスコでは、次のように修正済み拡張リリースにアップグレードすることを推奨しています。

- Cisco ISE が リリース 3.4 パッチ 2 を実行している場合、これ以上の操作は必要ありません。
- Cisco ISE が リリース 3.3 パッチ 6 を実行している場合、リリース 3.3 パッチ 7 で追加の修正が利用可能であり、デバイスをアップグレードする必要があります。
- Cisco ISE にホットパッチ ise-apply-CSCwo99449_3.3.0.430_patch4-SPA.tar.gz またはホットパッチ ise-apply-CSCwo99449_3.4.0.608_patch1-SPA.tar.gz のいずれかがインストール

されている場合、リリース 3.3 パッチ 7 またはリリース 3.4 パッチ 2 にアップグレードすることをお勧めします。このホットパッチは CVE-2025-20337 に対応していないため、CCO から保留されています。

Cisco ISE または ISE-PIC リリース	CVE-2025-20281 の最初の修正済みリリース	CVE-2025-20282 の最初の修正済みリリース	CVE-2025-20337 の最初の修正済みリリース
3.2 以前	脆弱性なし	脆弱性なし	脆弱性なし
3.3	3.3 パッチ 7	脆弱性なし	3.3 パッチ 7
3.4	3.4 パッチ 2	3.4 パッチ 2	3.4 パッチ 2

デバイスのアップグレード手順については、Cisco Identity Services Engine サポートページのアップグレードガイドを参照してください。

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

2025 年 7 月、Cisco PSIRT は、CVE-2025-20281 および CVE-2025-20337 の不正利用が実際に試みられたことを認識しました。これらの脆弱性が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、引き続き強くお勧めします。

出典

シスコは、これらの脆弱性を報告していただいた次の方々に感謝いたします。

- Trend Micro Zero Day Initiative の Bobby Gould 氏：CVE-2025-20281
- GMO サイバーセキュリティ by イエラエの川根健太郎氏が Trend Micro Zero Day Initiative: CVE-2025-20282 および CVE-2025-20337 に協力

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.2	不正利用の試みが確認された CVE を追加。	不正利用事例と公式発表	Final	2025年7月25日

バージョン	説明	セクション	ステータス	日付
2.1	実際に不正利用が試みられていることを示すように更新。	不正利用事例と公式発表	Final	2025 年 7 月 21 日
2.0	Cisco ISE コード修正を更新、CVE-2025-20337 を追加、CSCwp02814 を追加。	ヘッダー、サマリー、修正済みリリース	Final	2025 年 7 月 16 日
1.0	初回公開リリース	—	Final	2025 年 6 月 25 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。