Cisco Identity Services Engineにおける安全でないJavaデシリアライゼーションおよび許可バイパスの脆弱性

アドバイザリーID : cisco-sa-ise-multivuls-FTW9AOXF
初公開日 : 2025-02-05 16:00
バージョン 1.0 : Final
CVSSスコア : 9.9
回避策 : No workarounds available
Cisco バグ ID : CSCwk14916 CSCwk14901

CVE-2025-20124
CVE-2025-20125

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)の複数の脆弱性により、認証されたリモート攻撃者が任意のコマンドを実行し、該当デバイスの権限を昇格できる可能性があります。

注：これらの脆弱性をエクスプロイトするには、攻撃者は有効な読み取り専用管理クレデンシャルを持っている必要があります。

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。

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-multivuls-FTW9AOXF

該当製品

脆弱性のある製品

これらの脆弱性は、デバイス設定に関係なく、Cisco ISEおよびCisco ISE Passive Identity Connector(ISE-PIC)に影響を与えます。

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が存在する製品セクションにリストされている製品だけがこれらの脆弱性の影響を受けることが知られています。

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、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受ける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-2025-20124:Cisco ISEの安全でないJavaデシリアライゼーションの脆弱性

Cisco ISEのAPIの脆弱性により、認証されたリモート攻撃者が該当デバイスでルートユーザとして任意のコマンドを実行できる可能性があります。

この脆弱性は、該当ソフトウェアによるユーザ指定のJavaバイトストリームの安全でないデシリアライゼーションに起因します。攻撃者は、巧妙に細工されたシリアル化されたJavaオブジェクトを該当APIに送信することにより、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、攻撃者はデバイス上で任意のコマンドを実行し、権限を昇格できる可能性があります。

注：この脆弱性の不正利用に成功するには、攻撃者は有効な読み取り専用管理クレデンシャルを持っている必要があります。シングルノード展開では、リロード時に新しいデバイスを認証できません。

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。

バグID: CSCwk14916
CVE ID：CVE-2025-20124
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9.9
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H

CVE-2025-20125:Cisco ISE認可バイパスの脆弱性

Cisco ISEのAPIの脆弱性により、有効な読み取り専用クレデンシャルを持つ認証されたリモートの攻撃者が、機密情報を取得し、ノード設定を変更して、ノードを再起動する可能性があります。

この脆弱性は、特定のAPIでの認証の欠如と、ユーザが指定したデータの不適切な検証に起因します。攻撃者は、巧妙に細工された HTTP 要求をデバイス上の特定の API に送信することにより、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、情報を取得し、システム設定を変更し、デバイスをリロードすることができます。

注：この脆弱性の不正利用に成功するには、攻撃者は有効な読み取り専用管理クレデンシャルを持っている必要があります。シングルノード展開では、リロード時に新しいデバイスを認証できません。

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。

バグID: CSCwk14901
CVE ID：CVE-2025-20125
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9.1
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/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、およびこれら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 ISEソフトウェアリリース	First Fixed Release（修正された最初のリリース）
3.0	修正済みリリースに移行。
3.1	3.1P10
3.2	3.2P7
3.3	3.3P4
3.4	脆弱性なし

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

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された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とその公表は確認しておりません。

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。

- CVE-2025-20124:DeloitteのDan MarinおよびSebastian Radulea
- CVE-2025-20125:DeloitteのSebastian Radulea

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multivuls-FTW9AOXF

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2月5日

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。