# Cisco Identity Services Engine の脆弱性


アドバイザリーID : cisco-sa-ise-file-upload-FceLP4xs
初公開日 : 2023-11-01 16:00
バージョン 1.0 : Final
CVSSスコア : 4.7
回避策 : No workarounds available
Cisco バグ ID : CSCwc71225 CSCwd93720 CSCwd93717

CVE-2023-20196
CVE-2023-20195
CVE-2023-20213

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、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たり、Cisco Discovery Protocol(CDP)処理を無効にしたり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。

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-file-upload-FceLP4xs

## 該当製品

### 脆弱性のある製品

これらの脆弱性は Cisco ISE に影響を及ぼします。

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

これらの脆弱性の不正利用が可能なのは、Cisco ISEシステムの権限を持つユーザだけです。ベストプラクティスとして、コンソールアクセスと管理者Webアクセスを特定のIPアドレスまたは制限されたIPアドレスに制限できます。アクセス制限を設定するには、Webベースの管理インターフェイスを開き、Administration > System > Admin Access > Settings > Access > IP Accessの順に選択します。

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-2023-20195およびCVE-2023-20196:Cisco ISEの任意のファイルアップロードの脆弱性

Cisco ISEの2つの脆弱性により、認証された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できる可能性があります。これらの脆弱性をエクスプロイトするには、攻撃者は該当デバイスで有効な管理者クレデンシャルを持っている必要があります。

これらの脆弱性は、Webベースの管理インターフェイスにアップロードされたファイルの検証が不適切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、攻撃者は悪意のあるファイルをデバイスの特定のディレクトリに保存できる可能性があります。攻撃者は、後でこれらのファイルを使用して、影響を受けるデバイス上でルート権限を使用して任意のコードを実行するなど、追加の攻撃を実行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:CSCwd93717およびCSCwd93720
CVE ID：CVE-2023-20195 および CVE-2023-20196
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：4.7
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

CVE-2023-20213:Cisco ISE CDPのDoS脆弱性

Cisco ISEのCDP処理機能における脆弱性により、認証されていない隣接する攻撃者が、該当デバイスでCDPプロセスのサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、影響を受けるデバイスがCDPトラフィックを処理する際の境界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CDPトラフィックをデバイスに送信する

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。不正利用に成功すると、CDPプロセスがクラッシュし、ネイバー探索とリモートデバイスの到達可能性を判断するCisco ISEの機能に影響を与える可能性があります。クラッシュが発生した後、インターフェイスコンフィギュレーションモードでcdp enableコマンドを使用して、CDPプロセスを手動で再起動する必要があります。

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:CSCwc71225
CVE ID：CVE-2023-20213
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：4.3
CVSSベクトル：CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

## 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アップグレード ソリューション一式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。中央および右の列は、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 リリース | CVE-2023-20195 の最初の修正済みリリース<br>およびCVE-2023-20196 | CVE-2023-20213 の最初の修正済みリリース |
|---|---|---|
| 2.6 以前 | 修正済みリリースに移行。 | 修正済みリリースに移行。 |
| 2.7 | 2.7P10（日本未発売） | 2.7P10（日本未発売） |
| 3.0 | 3.0P8（2015年10月） | 3.0P7（2015年9月） |
| 3.1 | 3.1P8（2023年11月） | 3.1P6 |
| 3.2 | 3.2P3 | 3.2P2 |
| 3.3 | 脆弱性なし | 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 Services 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

CVE-2023-20195およびCVE-2023-20196：これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のArthur Vidineyevによる社内セキュリティテストで発見されました。

CVE-2023-20213：この脆弱性は、Cisco ASIGのX.B.による内部セキュリティテストで発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-upload-FceLP4xs

## 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 | 2023年11月1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。