

Cisco Identity Services Engineのコマンドインジェクションの脆弱性



アドバイザーID : [cisco-sa-ise-injection-QeXegrCw](#) [CVE-2023-20170](#)
初公開日 : 2023-11-01 16:00 [CVE-2023-20175](#)
バージョン 1.0 : Final [20175](#)
CVSSスコア : [8.8](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCwd07353](#) [CSCwd41220](#)

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、認証されたローカルの攻撃者が、基盤となるオペレーティングシステムに対してコマンドインジェクション攻撃を実行し、権限をrootに昇格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ーの「[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。

このアドバイザーは、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-injection-QeXegrCw>

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、このアドバイザーの「修正済みソフトウェア」セクションを参照してください。

脆弱性を含ま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、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-2023-20175 : Cisco ISE コマンドインジェクションの脆弱性

特定のCisco ISE CLIコマンドの脆弱性により、認証されたローカルの攻撃者が、基盤となるオペレーティングシステムに対してコマンドインジェクション攻撃を実行し、権限をrootに昇格できる可能性があります。こ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読み取り専用以上の権限を持っている必要があります。

この脆弱性は、ユーザ指定の入力の検証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CLIコマンドを送信することで、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 に特権昇格できるようになります。

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。

バグID:[CSCwd07353](#)

CVE ID : CVE-2023-20175

セキュリティ影響評価 (SIR) : 高

CVSS ベーススコア : 8.8

CVSS ベクトル : CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVE-2023-20170 : Cisco ISE コマンドインジェクションの脆弱性

特定のCisco ISE CLIコマンドの脆弱性により、認証されたローカルの攻撃者が、基盤となるオペレーティングシステムに対してコマンドインジェクション攻撃を実行し、権限をrootに昇格できる可能性があります。こ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権限を持っている必要があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、巧妙に細

与えられたCLIコマンドを送信することで、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 に特権昇格できるようになります。

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。

バグID:[CSCwd41220](#)

CVE ID : CVE-2023-20170

セキュリティ影響評価 (SIR) : 中

CVSS ベーススコア : 6.0

CVSSベクトル : CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

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ン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です。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-2023-20175 の最初の修正済みリリース	CVE-2023-20170 の最初の修正済みリリース
2.7 以前	2.7P10 (日本未発売)	脆弱性なし
3.0	3.0P8 (2015年10月)	脆弱性なし
3.1	3.1P6	脆弱性なし
3.2	3.2P1	3.2P3
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-2023-20175：この脆弱性は、Cisco Advanced Security Initiatives Group(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。

CVE-2023-20170：この脆弱性を報告していただいたDeloitte社のDan Marin氏に感謝いたします。シスコは、Cisco ASIGのEvan Pickard氏にも感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-QeXegrCw>

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

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、単独の転載や意識を施した場合、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。