Cisco Identity Services Engine の脆弱性

Medium

アドバイザリーID : cisco-sa-ise-multi-vuln-DBQdWRy
初公開日 : 2024-11-06 16:00
バージョン 1.0 : Final
CVSSスコア : 6.1
回避策 : No workarounds available
Cisco バグ ID : CSCwk47454 CSCwk47465 CSCwk47475 CSCwk47423 CSCwk47445 CSCwk47489 CSCwk47451

CVE-2024-20531
CVE-2024-20530
CVE-2024-20532
CVE-2024-20525
CVE-2024-20528
CVE-2024-20527
CVE-2024-20529

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、リモート攻撃者がWebベース管理インターフェイスのユーザに対してクロスサイトスクリプティング(XSS)攻撃を実行したり、パストラバーサル攻撃を実行したり、該当デバイス上の任意のファイルを読み取って削除したり、デバイスを介してサーバサイドリクエストフォージェリ(SSRF)攻撃を実行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-multi-vuln-DBQdWRy

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性はデバイス設定に関係なくCisco ISEに影響を与えました。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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-2024-20525およびCVE-2024-20530:Cisco ISEの反映クロスサイトスクリプティングの脆弱性

Cisco ISEのWebベース管理インターフェイスにおける2つの脆弱性により、認証されていないリモートの攻撃者がインターフェイスのユーザに対してXSS攻撃を実行する可能性があります。

これらの脆弱性は、Webベースの管理インターフェイスがユーザ入力を適切に検証しないことに起因しています。攻撃者は、インターフェイスのユーザが巧妙に細工されたリンクをクリックするように仕向けることで、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、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセス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: CSCwk47423、CSCwk47454
CVE ID: CVE-2024-20525、CVE-2024-20530
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE-2024-20527、CVE-2024-20529、およびCVE-2024-20532:Cisco ISEにおける任意ファイルの読み取りおよび削除に関する脆弱性

Cisco ISEのAPIにおける3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で任意のファイルを読み取って削除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、攻撃者は有効なスーパー管理者クレデンシャルを必要とします。

これらの脆弱性は、API要求におけるユーザ指定パラメータの検証が不十分であることに起因します。攻撃者は、該当デバイスに巧妙に細工されたAPI要求を送信することにより、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、攻撃者は基盤となるオペレーティングシステム上の任意のファイルの読み取りまたは削除を実行でき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: CSCwk47489、CSCwk47445、CSCwk47475
CVE ID: CVE-2024-20527、CVE-2024-20529、CVE-2024-20532
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.5
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N

CVE-2024-20531:Cisco ISE XML外部エンティティインジェクションの脆弱性

Cisco ISEのAPIにおける脆弱性により、認証されたリモートの攻撃者が、該当デバイスの基盤となるオペレーティングシステム上で任意のファイルを読み取り、該当デバイスを介してサーバ側の要求フォージェリ(SSRF)攻撃を実行する可能性があります。この脆弱性を不正利用するには、攻撃者は有効なスーパー管理者クレデンシャルを必要とします。

この脆弱性は、XML入力を解析する際のXML外部エンティティ(XXE)エントリの不適切な処理に起因します。攻撃者は、巧妙に細工された API 要求を該当デバイス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、攻撃者は基盤となるオペレーティングシステム上の任意のファイルを読み取ったり、該当デバイスを介してSSRF攻撃を実行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:CSCwk47465
CVE ID：CVE-2024-20531
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.5
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N

CVE-2024-20528:Cisco ISEのパストラバーサルの脆弱性

Cisco ISEのAPIにおける脆弱性により、認証されたリモート攻撃者が、該当デバイスの基盤となるオペレーティングシステム上の任意の場所にファイルをアップロードできる可能性があります。この脆弱性を不正利用するには、攻撃者は有効なスーパー管理者クレデンシャルを必要としま

す。

この脆弱性は、API要求のユーザ指定パラメータ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 API 要求を該当デバイス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、攻撃者はカスタムファイルを基盤となるオペレーティングシステムの任意の場所にアップロードし、任意のコードを実行して、権限をrootに昇格することができます。

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:CSCwk47451
CVE ID：CVE-2024-20528
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：3.8
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/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

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。

修正済みリリース

発行時点では、次の表に記載されているリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列には、シスコソフトウェアリリースが一覧表示されます。中央と右側の列は、リリースがこれらの脆弱性の影響を受けたかどうか、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。

Cisco ISE リリース	CVE-2024-20528、CVE-2024-20529の最初の修正済みリリース	CVE-2024-20525、CVE-2024-20527、CVE-2024-20530、CVE-2024-20531、CVE-2024-20532の最初の修正済みリリース
3.0 以前	脆弱性なし	修正済みリリースに移行。
3.1	3.1P10（2025年1月）	3.1P10（2025年1月）
3.2	3.2P7	3.2P7
3.3	3.3P4	3.3P4
3.4	脆弱性なし	3.4P1（2024年11月）

デバイスのアップグレード手順については、Cisco Identity Service Engineサポートページの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-2024-20525、CVE-2024-20527、CVE-2024-20528、CVE-2024-20529、CVE-2024-20530、CVE-2024-20531、CVE-2024-20532：これらの脆弱性を報告していただいたセキュリティ研究者Pear1yに感謝いたします。

CVE-2024-20527：この脆弱性を個別に報告していただいたIeraeのGMO Cybersecurityの川根健太郎氏にも感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-vuln-DBQdWRy

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	2024年11月6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。