Cisco Identity Services Engineの権限昇格の脆弱性

アドバイザリーID : cisco-sa-ise-priv-esc-KJLp2Aw
初公開日 : 2023-09-06 16:00
最終更新日 : 2024-01-08 19:01
バージョン 1.2 : Final
CVSSスコア : 6.0
回避策 : No workarounds available
Cisco バグ ID : CSCwd93721 CSCwd07348

CVE-2023-20194
CVE-2023-20193

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、認証された攻撃者が権限昇格攻撃を実行し、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変更したりす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、攻撃者は影響を受けるデバイスに対する有効な管理者レベルの権限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のいずれか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-priv-esc-KJLp2Aw

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Cisco ISEに影響を与えました。

CVE-2023-20193で説明されている脆弱性は、Cisco ISEの脆弱性が存在するリリースを実行し、Embedded Service Router(ESR)を有効にしているシスコデバイスに影響を与えます。

CVE-2023-20194で説明されている脆弱性は、Cisco ISEの脆弱性が存在するリリースを実行し、外部RESTfulサービス(ERS)を有効にしているシスコデバイスに影響を与えます。

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

これらの脆弱性は互いに依存していないため、一方の脆弱性を悪用しても他方の脆弱性を悪用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。

注：これらの脆弱性の不正利用が可能なのは、Cisco ISEの有効な認証ユーザのみです。ベストプラクティスとして、お客様はコンソールアクセスと管理 Web アクセスを制限できます。アクセス制限を設定するには、Administration > System > Admin Access > Settings > Access > IP Accessの順に選択します。

脆弱性の詳細は以下のとおりです。

CVE-2023-20193:Cisco ISEの権限昇格の脆弱性

Cisco ISEのEmbedded Service Router(ESR)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上で任意のファイルを読み取り、書き込み、または削除し、権限をrootに昇格できる可能性があります。この脆弱性を工クスプロイトするには、攻撃者は影響を受けるデバイスに対する有効な管理者レベルの権限を持っている必要があります。

この脆弱性は、ESRコンソールでの不適切な権限管理に起因します。細工された要求が該当デバイスに送信されると、この脆弱性が工クスプロイトされる危険性があります。工クスプロイトに成功すると、攻撃者は権限をrootに昇格し、該当デバイスの基盤となるオペレーティングシステムから任意のファイルを読み取り、書き込み、または削除できる可能性があります。

注：ESRはデフォルトでは有効になっていないため、ライセンスが必要です。Admin GUIでESRのステータスを確認するには、Administration > Settings > Protocols > IPSecの順に選択します。

この脆弱性に対処する回避策はありません。

バグID:CSCwd07348
CVE ID：CVE-2023-20193

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

CVE-2023-20194:Cisco ISEの権限昇格の脆弱性

Cisco ISEのERS APIの脆弱性により、認証されたリモートの攻撃者が、該当デバイスの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、攻撃者は影響を受けるデバイスに対する有効な管理者レベルの権限を持っている必要があります。

この脆弱性は、ERS APIの不適切な権限管理に起因します。細工された要求が該当デバイスに送信されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、攻撃者は意図したアクセスレベルを超えて権限を昇格させ、基盤となるオペレーティングシステム(OS)から機密情報を取得できる可能性があります。

注：ERSはデフォルトでは有効になっていません。Admin GUIでERS APIのステータスを確認するには、Administration > Settings > API Settings > API Service Settingsの順に選択します。

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:CSCwd93721
CVE ID：CVE-2023-20194
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.9
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/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、次の表に示す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。

Cisco ISE リリース	CVE-2023-20193 の最初の修正済みリリース	CVE-2023-20194 の最初の修正済みリリース
2.7 以前	計画なし.	2.7P10
3.0	計画なし.	3.0P8
3.1	計画なし.	3.1P8
3.2	計画なし.	3.2P3
3.3	計画なし.	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-2023-20193：この脆弱性は、Cisco Advanced Security Initiatives Group（ASIG）の X.B. によるシスコ内部のセキュリティテストで発見されました。

CVE-2023-20194：この脆弱性は、Cisco ASIGのArthur Vidineyev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-priv-esc-KJLp2Aw

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	修正済みリリースの表を更新。	修正済みリリース	Final	2024年1月8日

バージョン	説明	セクション	ステータス	日付
1.1	修正済みリリースの目標期日を追加。	修正済みリリース	Final	2023年9月8日
1.0	初回公開リリース	—	Final	2023 年 9 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。