Cisco Identity Services Engineの機密情報の漏えいの脆弱性

Medium

アドバイザリーID : cisco-sa-ise-info-exp-vdF8Jbyk
CVE-2024-20466
初公開日 : 2024-08-21 16:00
最終更新日 : 2024-09-05 13:14
バージョン 1.1 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwh78725 CSCwe48929

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Webベースの管理インターフェイス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から機密情報を取得できる可能性があります。

この脆弱性は、高価値の機密データに対する管理特権レベルの不適切な適用に起因します。影響を受けるデバイスのWebベース管理インターフェイスで読み取り専用の管理者権限を持つ攻撃者が、機密データが含まれているページを参照することで、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、攻撃者はシステムの設定に関する機密情報を収集できる可能性があります。

シスコはCSCwh78725に対処するソフトウェアアップデートをリリースしました。シスコでは、CSCwe48929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せん。こ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-info-exp-vdF8Jbyk

該当製品

脆弱性のある製品

公開時点で、この脆弱性は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、この脆弱性の影響を受けることが分かっています。

回避策

こ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。

左側の列にはシスコソフトウェアリリース、右側の列に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、およびこの脆弱性に対する修正を含むリリースが示されています。

Cisco ISE リリース	第1修正済みリリース(CSCwh78275)
2.7 以前	修正済みリリースに移行。
3.0	修正済みリリースに移行。
3.1	3.1P10
3.2	3.2P5
3.3	3.3P2
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 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やその公表は確認しておりません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-exp-vdF8Jbyk

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	緩和情報を削除し、リリース3.1の修正済みリリースを追加。	「回避策」および「修正済みリリース」	Final	2024年9月5日
1.0	初回公開リリース	—	Final	2024 年 8 月 21 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。