Cisco Identity Services Engine REST APIブラインドSQLインジェクションの脆弱性

Medium

アドバイザリーID : cisco-sa-ise-rest-5bPKrNtZ
初公開日 : 2024-08-21 16:00
最終更新日 : 2024-08-22 15:15
バージョン 1.1 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwj94297 CSCwj94294 CSCwj94315 CSCwj94305

CVE-2024-20417

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REST APIの複数の脆弱性により、認証されたリモートの攻撃者がブラインドSQLインジェクション攻撃を実行できる可能性があります。

これらの脆弱性は、REST APIコールにおけるユーザ入力の検証が不十分であることに起因します。攻撃者は、巧妙に細工された入力を該当デバイスに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、攻撃者は該当デバイスのデータを表示または変更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。

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-rest-5bPKrNtZ

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。

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。

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。

左の列にはCiscoソフトウェアリリースが、右の列にはそのリリースが本アドバイザリに記載された脆弱性の影響を受けるかどうか、またどのリリースにこれらの脆弱性に対する修正が含まれているかを示します。

Cisco ISE リリース	First Fixed Release（修正された最初のリリース）
3.0 以前	修正済みリリースに移行。
3.1	3.1パッチ10（2025年1月）
3.2	3.2パッチ7（2024年9月）
3.3	3.3パッチ4（2024年10月）
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とその公表は確認しておりません。

出典

これらの脆弱性を報告していただいたGMO Cybersecurity by Ieraeの川根健太郎氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rest-5bPKrNtZ

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	将来の修正済みリリースを含むように表を更新。	修正済みリリース	Final	2024年8月22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。