

Cisco Smart Licensing Utility の脆弱性



アドバイザーID : cisco-sa-cslu-7gHMzWmw

初公開日 : 2024-09-04 16:00

最終更新日 : 2025-04-04 17:44

バージョン 1.2 : Final

CVSSスコア : [9.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwi47950](#) [CSCwi41731](#)

[CVE-2024-](#)

[20440](#)

[CVE-2024-](#)

[20439](#)

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 Smart Licensing Utility の複数の脆弱性により、認証されていないリモートの攻撃者が、ソフトウェアの実行中に機密情報を収集したり、システム上の Cisco Smart Licensing Utility サービスを管理したり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。

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-cslu-7gHMzWmw>

該当製品

脆弱性のある製品

これらの脆弱性は、ソフトウェア設定に関係なく、Cisco Smart Licensing Utility の脆弱なリリースを実行しているシステムに影響を与えます。

注：これらの脆弱性は、Cisco Smart Licensing Utilityがユーザによって開始され、アクティブに実行されていない限り、不正利用されることはありません。

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。

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- Smart Software Manager オンプレミス
- Smart Software Manager サテライト

詳細

これらの脆弱性は依存関係ではなく、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-2024-20439 : Cisco Smart Licensing Utility の静的なログイン情報の脆弱性

Cisco Smart Licensing Utility の脆弱性により、認証されていないリモートの攻撃者が静的な管理者ログイン情報を使用して、該当システムにログインする可能性があります。

この脆弱性は、管理アカウントの文書化されていない静的なユーザーログイン情報に起因します。攻撃者は、静的なログイン情報を使用して該当システムにログインすることで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は Cisco Smart Licensing Utility アプリケーションの API に対して管理者権限で該当システムにログインでき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: [CSCwi41731](#)

CVE ID : CVE-2024-20439

セキュリティ影響評価 (SIR) : 致命的

CVSS ベーススコア : 9.8

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

CVE-2024-20440 : Cisco Smart Licensing Utility の情報漏洩の脆弱性

Cisco Smart Licensing Utility の脆弱性により、認証されていないリモートの攻撃者が機密情報にアクセスできる可能性があります。

この脆弱性は、デバッグログファイルの過剰な冗長性に起因します。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、この脆弱性を不正利用する可能性があります。

す。不正利用に成功すると、攻撃者は API へのアクセスに使用できるログイン情報を含む、機密データを含むログファイルを取得でき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: [CSCwi47950](#)

CVE ID : CVE-2024-20440

セキュリティ影響評価 (SIR) : 致命的

CVSS ベーススコア : 9.8

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

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完全なアップグレード ソリューション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。右の列は、リリースがこれらの脆弱性の影響を受けているかどうか、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 Smart License Utility リリース	First Fixed Release (修正された最初のリリース)
2.0.0	修正済みリリースに移行。
2.1.0	修正済みリリースに移行。
2.2.0	修正済みリリースに移行。
2.3.0	脆弱性なし

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

2025年3月、Cisco Product Security Incident Response Team(PSIRT)は、CVE-2024-20439の不正利用が試みられていることを認識しました。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

出典

この脆弱性は、シスコ内部でのシステムセキュリティテスト中に、シスコの Eric Vance によって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw>

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	不正利用されたことが判明している特定のCVEを追加。	不正利用事例と公式発表	Final	2025年4月4日
1.1	シスコが不正利用を認識したことを反映するように更新。	不正利用事例と公式発表	Final	2025年4月1日
1.0	初回公開リリース	—	Final	2024 年 9 月 4 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。