

Cisco License(Smart Software Manager)オンプレミスの脆弱性



Advisory ID : cisco-sa-ssm-access-nttb2dhE [CVE-2026-](#)

初公開日 : 2026-10-07 16:00

[76454](#)

バージョン 1.0 : Final

[CVE-2026-](#)

CVSSスコア : [9.1](#)

[20328](#)

回避策 : No workarounds available

[CVE-2026-](#)

Cisco Bug ID : [CSCwv53803](#) [CSCwv53814](#) [76452](#)

[CSCwu54774](#) [CSCwv53807](#)

[CVE-2026-](#)

[76437](#)

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

Cisco License On-Prem(旧称Cisco Smart Software Manager On-Prem(SSM On-Prem))のWebベース管理インターフェイスおよびAPIエンドポイントの複数の脆弱性により、リモート攻撃者が不正アクセス、機密情報へのアクセス、サービス妨害(DoS)状態の発生、または権限の昇格を行う可能性があります。

これらの脆弱性の詳細については、このアドバイザリの「[詳細情報](#)」の項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-ssm-access-nttb2dhE>

オンプレミスのシスコライセンスの改善と修正に関するその他のドキュメントについては、「[オンプレミスのセキュリティ強化リリース: シスコライセンス\(Smart Software Manager\)](#)」を参照してください。

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、オンプレミスのシスコライセンスに影響します。このソフトウェアの以前のリリースはCisco SSM On-Premと呼ばれ、これらも該当しま

す。

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。

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Cisco Smart Licensing Utilityには影響を与えないことを確認しました。

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別の脆弱性をエクスプロイトする必要はありません。また、これらの脆弱性のいずれかに該当するソフトウェアリリースでも、他の脆弱性には該当しない可能性があります。

脆弱性の詳細は以下のとおりです。

CVE-2026-20328: Cisco License(Smart Software Manager)のオンプレミスでの任意アカウントのパスワードリセットの脆弱性

Cisco License On-Prem(旧称Cisco Smart Software Manager On-Prem(SSM On-Prem))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、認証されていないリモートの攻撃者が該当アプリケーションに不正アクセスする可能性があります。

この脆弱性は、パスワードリセットプロセス中の不適切なチェックに起因します。攻撃者は、Web ベース管理インターフェイスに悪意のある要求を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、高特権の管理ユーザーアカウントを含む任意のアカウントのパスワードをリセットし、任意のユーザーとしてアプリケーションへの不正アクセスを取得する可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: [CSCwv53803](#)

CVE ID : CVE-2026-20328

セキュリティ影響評価 (SIR) : 致命的

CVSS ベーススコア : 9.1

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

CVE-2026-76454 : シスコライセンス(Smart Software Manager)のオンプレミス非認証APIの脆弱性

Cisco License On-Prem(以前のCisco Smart Software Manager On-Prem(SSM On-Prem))のCisco Smart Licensing Utility APIの脆弱性により、認証されていないリモートの攻撃者がシステムに任意のファイルを書き込んだり、該当アプリケーションでDoS状態を引き起こしたりする可能性があります。

この脆弱性は、入力の検証が不適切で、管理APIでの認証が行われないことに起因します。攻撃者は、細工された要求を該当API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、攻撃者はシステムファイルを変更したり、DoS状態を引き起こしたりする可能性があります。

この脆弱性に対処するソフトウェアアップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: [CSCwu54774](#)

CVE ID : CVE-2026-76454

セキュリティ影響評価 (SIR) : 致命的

CVSS ベーススコア : 9.1

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

CVE-2026-76437: Cisco License(Smart Software Manager)オンプレミスのコマンドインジェクションの脆弱性

Cisco License On-Prem(旧称Cisco Smart Software Manager On-Prem(SSM On-Prem))のWebベースのユーザ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基盤となるオペレーティングシステムで任意のコマンドを実行する可能性があります。

この脆弱性は、Webベースの管理インターフェイスに送信された設定内で、ユーザが指定したコンテンツの検証が不適切なことに起因します。攻撃者は、Webベースの管理インターフェイス内で設定を更新することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はroot権限を使用して、基盤となるオペレーティングシステムで任意のコマンドを実行でき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、攻撃者は有効な管理者ログイン情報を持っている必要があります。この脆弱性を悪用できるのは、システム管理者権限を持っている攻撃者に限られます。そのため、システムの電源を切る機能を追加する権限は、管理ユーザには通常は与えられません。

この脆弱性に対処するソフトウェアアップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: [CSCwv53807](#)

CVE ID : CVE-2026-76437

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:N/I:N/A:H

CVE-2026-76452: Cisco License(Smart Software Manager)オンプレミスSQLインジェクションの脆弱性

Cisco License On-Prem(旧称Cisco Smart Software Manager On-Prem(SSM On-Prem))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、該当アプリケーションに対してSQLインジェクション攻撃を実行する可能性があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、Webベース管理インターフェイスに細工された要求を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、影響を受けるアプリケーションの内部データベースで、通常はアクセスできない追加のコンテンツを読み取り、システムの機密性に影響を与える可能性があります。

この脆弱性を不正利用するには、攻撃者は該当アプリケーションで有効な管理ユーザクレデンシャルを持っている必要があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: [CSCwv53814](#)

CVE ID : CVE-2026-76452

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

シスコでは、回避策や緩和策 (該当する場合) は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正リリース

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ライセンスオンプレミスリリース	第 1 修正済みリリース
9-202601以前 ¹	修正済みリリースに移行。
10-202608 より前	10-202608
10-202609	脆弱性なし

1. これらのリリースのシスコライセンスは、Cisco Smart Software Manager On-Premと呼ばれていました。アップグレードおよび移行の詳細については、[シスコライセンスオンプレミスリリースノート](#)を参照してください。

シスコの 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済み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。

送信元

これらの脆弱性を報告していただいた以下の研究者の方々に感謝いたします。

- NATOサイバーセキュリティセンター(NCSC)のGabriele Paris氏：CVE-2026-20328、CVE-2026-76437、およびCVE-2026-76452
- CyStackのTrung Nguyen(@everping):CVE-2026-76454

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-access-nttb2dhE>

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2026年10月7日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

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。お客様がソフトウェアをダウンロードでき

るのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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 Technical Assistance Center \(TAC \)](#) 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。

[ソフトウェアのアップグレードを検討する](#) 際には、関連するシスコ製品の[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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、[シスコ セキュリティ アドバイザリ](#) ページをご覧ください。Cisco 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済みリリース情報のみを評価します。詳細については、[シスコのセキュリティ脆弱性ポリシー](#)を参照してください。

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。