

Cisco Secure Workload ソフトウェアのセキュリティ強化リリース：2026 年 8 月



アドバイザリーID : cisco-sa-hardening-

csw1-shSvndWP

初公開日 : 2026-08-19 16:00

バージョン 1.0 : Final

CVSSスコア : [10.0](#)

回避策 : No workarounds available

Cisco バグ ID :

[CVE-2026-20318](#)

[CVE-2026-20319](#)

[CVE-2026-20317](#)

[CVE-2026-20315](#)

[CVE-2026-20231](#)

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

プロアクティブなセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、シスコセキュアワークロードエンジニアリングチームは、包括的な社内セキュリティレビューを実施しました。このレビューの結果、社内で見つめられた複数の脆弱性に対処するソフトウェアのセキュリティ強化リリースが公開されました。

これらの脆弱性は内部テストで見つめられたものであり、現時点でエクスプロイトの事例は確認されていません。お客様によるパッチ適用を支援し、開示プロセスを効率化するために、シスコはこれらの問題をその根本的な脆弱性クラス (Common Weakness Enumeration (CWE)) ごとに分類し、CWE の各グループに 1 つの共通脆弱性識別子 (CVE ID) を割り当てました。

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-hardening-csw1-shSvndWP>

該当製品

脆弱性のある製品

これらの脆弱性は、デバイスの設定に関係なく、Cisco Secure Workload Software as a Service(SaaS)およびオンプレミス展開に影響を与えます。

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。

詳細

次の表に、これらの強化リリースで対処されている脆弱性クラスの概要を示します。各 CVE ID に割り当てられる CVSS スコアは、その特定の CWE カテゴリ内で最も影響の大きい 1 つの根本的な脆弱性がもたらす可能性がある最大のシビラティ（重大度）を表しています。

CVE ID	CVSS最高スコア	脆弱性クラス (最高レベルの CWE)	説明
CVE-2026-20231	9.9	CWE-74	特殊要素の不適切な無効化 (コマンド、OS、引数インジェクションなど)
CVE-2026-20315	10	CWE-284	不適切なアクセス制御 (承認、認証、権限、およびバイパスなど)
CVE-2026-20317	10	CWE-287	不適切な認証 (認証の欠落、認証バイパス、および信頼できない入力への依存を含む)
CVE-2026-20318	9.6	CWE-20	不適切な入力検証 (入力検証、パストラバースル、外部パス制御など)
CVE-2026-20319	7.5	CWE-119	メモリバッファの範囲内での操作の不適切な制限 (バッファのオーバーフローと範囲外の書き込みなど)

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

これらの脆弱性を完全に修正し、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。右側の列は、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 Secure Workload リリース	First Fixed Release (修正された最初のリリース)
3.10 以前	3.10.9.1
4.0	4.0.4.16

注：これらの脆弱性をすべて解決するには、Cisco Secure Workload のクラスタ、エージェント、およびコネクタのソフトウェアをアップグレードする必要があります。SaaS 展開の場合、シスコはクラスタソフトウェアをアップグレード済みであり、お客様は、エージェントとコネクタのソフトウェアのみをアップグレードする必要があります。

ソフトウェアのアップグレードに関する追加情報が必要な場合は、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。

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。

出典

これらの脆弱性は、既存のテストプロセスおよびフロンティアの AI モデルを使用した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-hardening-csw1-shSvndWP>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2026 年 8 月 19 日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。