

# Cisco Secure Workloadの不正なAPIアクセスの脆弱性



アドバイザーID : cisco-sa-csw-pnbsa-g8WEnuy [CVE-2026-20223](#)  
初公開日 : 2026-05-20 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 : [CSCwt99942](#)

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 Secure Workloadの内部REST APIのアクセス検証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、Site Adminロールの権限を使用してサイトリソースにアクセスできる可能性があります。

この脆弱性は、REST APIエンドポイントにアクセスする際の不十分な検証および認証に起因します。攻撃者は、巧妙に細工されたAPI要求を該当エンドポイントに送信できる場合、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、サイト管理者ユーザの権限を使用して、テナントの境界を越えて機密情報を読み取り、設定を変更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。

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-csw-pnbsa-g8WEnuy>

## 該当製品

### 脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、SaaSおよびオンプレミスの導入におけるCisco Secure Workload Clusterソフトウェアに影響を与えます。

注：この脆弱性は、内部REST APIのみに影響し、Webベースの管理インターフェイスには影

響しません。

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](#)にリストされている製品だけがこの脆弱性の影響を受けることが知られています。

## 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

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)
3.9 以前	修正済みリリースに移行。
3.10	3.10.8.3
4.0	4.0.3.17

シスコは、クラウドベースのCisco Secure Workload SaaS導入でこの脆弱性に対処しています。ユーザの対処は必要ありません。

その他の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やその公表は確認しておりません。

## 出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csw-pnbsa-g8WEnuy>

## 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5月20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。