Cisco Crosswork 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-crosswork-UzDTU9Vh
初公開日 : 2026-08-19 16:00
最終更新日 : 2026-08-21 16:54
バージョン 2.0 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID :

CVE-2026-20030
CVE-2026-20358
CVE-2026-20359
CVE-2026-20357

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、Cisco Crosswork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。このレビュー結果、社内で発見さ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発見されたものであり、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-crosswork-UzDTU9Vh

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、次のCisco Crossworkプラットフォームに影響を与えます。

- Crosswork Data Gateway
- Crosswork Network Controller
- クロスワーク計画
- Crossworkワークフローマネージャー

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-2026-20030	10.0	CWE-89	SQLコマンドで使用される特殊要素の不適切な無効化
CVE-2026-20357	10.0	CWE-306	重要な機能に対する認証の欠如
CVE-2026-20358	10.0	CWE-73	ファイルシステムの外部制御
CVE-2026-20359	9.9	CWE-522	ログイン情報の保護が不十分

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

以下の表では、左の列に Cisco Crosswork 製品が記載されています。中央の列には、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具体的なリリースが示されています。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 Crosswork 製品	Cisco Crosswork リリース	First Fixed Release（修正された最初のリリース）
Crosswork Data Gateway	7.2.1 以前	7.2.1- SP
Crosswork Network Controller	7.2.1 以前	7.2.1- SP
Crosswork Planning	7.2.1 以前	7.2.1- SP
Crosswork Workflow Manager	2.1.1 以前	2.1.1 - SP

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-crosswork-UzDTU9Vh

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.0	影響を受ける製品に Cisco Crosswork Workflow Manager を追加。	「脆弱性のある製品」および「修正済みリリース」	Final	2026 年 8 月 21 日
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。