Cisco IOS XE 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-iosxe-V8NMuMZJ
初公開日 : 2026-08-05 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID :

CVE-2026-20271
CVE-2026-20272
CVE-2026-20270
CVE-2026-20268
CVE-2026-20269
CVE-2026-20267
CVE-2026-20273

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

予防的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 IOS XEソフトウェア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-iosxe-V8NMuMZJ

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、自律モードまたはコントローラモードで実行されている Cisco IOS XE ソフトウェアに影響を及ぼします。

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。

注：この評価は、Cisco IOS XE ソフトウェアリリース 17.9、17.12、17.15、17.18、および 26.1 を対象としています。Cisco Catalyst 3650 および 3850 シリーズ スイッチでは、これらのリリースは実行されていないため、このレビューの一部として評価されていません。Cisco Catalyst 3650 および 3850 シリーズ スイッチに影響を与えることが確認されている脆弱性は、公開されているセキュリティ脆弱性ポリシーに記載されているとおり、将来のリリースで修正されることになっています。

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。

詳細

次の表に、これらのソフトウェア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 つの根本的なバグ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-2026-20267	9.0	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-2026-20268	8.6	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）
CVE-2026-20269	8.6	CWE-664	ライフタイム期間中のリソースの不適切な制御（メモリおよびファイルハンドラ、Null ポインタの逆参照、無効な解放など）
CVE-2026-20270	8.6	CWE-682	不正な計算（整数オーバーフロー、アンダーフロー、切り捨てなどの演算エラーまたは数値変換エラーなど）

CVE ID	CVSS最高スコア	脆弱性クラス（最高レベルのCWE）	説明
CVE-2026-20271	8.6	CWE-691	不十分な制御フロー管理（無限ループ、制御不能な再帰、競合状態など）
CVE-2026-20272	9.8	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-2026-20273	8.6	CWE-20	不適切な入力検証（入力検証、パストラバーサル、外部パス制御など）

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 IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
17.9	17.9.10
17.12	17.12.8
17.15	17.15.6
17.18	17.18.4、17.18.4a
26.1	26.1.2

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-iosxe-V8NMuMZJ

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 5 日

利用規約

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。