# Cisco IOS XRソフトウェアのセキュリティ強化リリース：2026年9月

Critical

アドバイザリーID : cisco-sa-hardening-iosxr-qg64NcM
初公開日 : 2026-09-02 16:00
最終更新日 : 2026-09-04 18:57
バージョン 1.3 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID :

CVE-2026-20280
CVE-2026-20279
CVE-2026-20277
CVE-2026-20278
CVE-2026-20275
CVE-2026-20276
CVE-2026-20274

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 XR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-iosxr-qg64NcM

# 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 IOS XR7(LNT)ソフトウェアを含むすべてのCisco IOS XRソフトウェアリリースに影響を与えます。

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。

デバイスがCisco IOS XR7(LNT)ソフトウェアを実行しているかどうかの確認

デバイスがCisco IOS XR7(LNT)ソフトウェアを実行しているかどうかを確認するには、show versionコマンドを使用します。次の例に示すように、コマンドからLNTを含む出力が返された場合、デバイスはCisco IOS XR7(LNT)ソフトウェアを実行しています。

<#root>

```
RP/0/RP0/CPU0:Router#show version
Tue Sep 1 05:44:27.305 UTC
Cisco IOS XR Software, Version 24.3.2
LNT

RP/0/RP0/CPU0:Router#
```

## 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-2026-20274 | 9.8 | CWE-664 | リソースの不適切な制御（入力サイズをチェックしないバッファコピー、スタックベースのバッファオーバ |

| CVE ID | CVSS最高スコア | 脆弱性クラス（最高レベルのCWE） | 説明 |
| --- | --- | --- | --- |
| | | | ーフロー、ヒープベースのバッファオーバーフロー、範囲外の読み取り、外部で制御されたフォーマット文字列の使用、数値切り捨てエラー、解放後のリソースの使用、期限切れまたは解放後のリソースの操作、制限またはスロットリングなしのリソースの割り当て、範囲外の書き込み、範囲外のポインタオフセットの使用、安全デフォルトをのリソースのの初期化） |
| CVE-2026-20275 | 8.8 | CWE-682 | 不正確な計算(バッファサイズの不正確な計算、整数オーバーフローまたはラップアラウンド、および整数アンダーフロー（ラップまたはラップアラウンド）を対象とする) |
| CVE-2026-20276 | 8.6 | CWE-691 | 不十分な制御フロー管理（到達可能なアサーションおよび到達不能な終了条件を持つループをカバー） |
| CVE-2026-20277 | 8.2 | CWE-693 | 保護メカニズムの障害（不適切なランダム値の使用をカバー） |
| CVE-2026-20278 | 8.8 | CWE-707 | 不適切な無害化（コマンドで使用される特殊要素の不適切な無害化、動的に評価されるコードのディレクティブの不適切な無害化、配列索引の不適切な検証、入力中の指定された数量の不適切な検証、および入力中の指定された索引、位置またはオフセットの不適切な検証を含む） |
| CVE-2026-20279 | 9.8 | CWE-284 | 不適切なアクセス制御（不適切な証明書の検証、重要な機能に対する認証の欠如、認可の欠如、および不正な認可を含む） |
| CVE-2026-20280 | 8.8 | CWE-703 | 例外的な状況に対する不適切なチェックまたは処理（長さパラメータの不整合に対する不適切な処理および安全に失敗しない処理をカバー） |

## 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

これらの脆弱性を修正し、本アドバイザリに記載されている障害の発生を回避するために、お客様には本アドバイザリに記載の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、左の列に該当するCisco IOS XRソフトウェアトレインを、右の列にこれらの脆弱性に対処するための該当プラットフォームのSMUが割り当てられているリリース、または今後のリリースに修正が含まれるリリースを示します。

表に基づいて、次のアクションを実行することをお勧めします。

1. 使用可能なSMUがあるリリースにアップグレードします。
2. アップグレードされたリリースに適切なSMUを適用します。

このアドバイザリのCWEでカバーされている脆弱性を緩和するために、各リリースで約16のSMUを使用できる可能性があります。今後のCisco IOS XRソフトウェアリリース26.2.2および26.3.1は、SMUを必要としない最初の修正済みリリースになる予定です。

| Cisco IOS XRソフトウェアトレイン | 最初の修正済みリリースとSMUの可用性 |
|---|---|
| 7.3（光ファイバのみ） | 7.3.2[1]で使用可能なSMU |
| 7.9 | 7.9.2および7.9.21で使用可能なSMU |
| 7.10 | 7.10.2で使用可能なSMU |
| 7.11 | 7.11.2および7.11.21で使用可能なSMU |
| 24.1 | 24.1.2用のSMU（今後のリリース） |
| 24.2 | 24.2.2および24.2.21で使用可能なSMU |
| 24.3 | 24.3.2用のSMU（今後のリリース） |
| 24.4 | 24.4.2で使用可能なSMU |
| 25.1 | 25.1.2用のSMU（今後のリリース） |
| 25.2 | 25.2.21で使用可能なSMU<br>25.2.2用のSMU（今後のリリース） |
| 25.4（光ファイバのみ） | 25.4.1[2]で使用可能なSMU |
| 25.4（オプティカル以外） | 25.4.2で使用可能なSMU |
| 26.1 | 26.1.2で使用可能なSMU |

| Cisco IOS XRソフトウェアトレイン | 最初の修正済みリリースとSMUの可用性 |
|---|---|
| 26.2 | 26.2.1で使用可能なSMU<br>26.2.2 (future release) |
| 26.3 | 26.3.1 (future release) |

1. リリース7.3.2のSMUは、光プラットフォームCisco Network Convergence System(NCS)1002でのみ使用できます。
2. リリース25.4.1のSMUは、光プラットフォームCisco NCS 1001、Cisco NCS 1004、およびCisco NCS 1010でのみ使用できます。

上記の表に記載されていないリリースでSMUを必要とするお客様は、Cisco Technical Assistance Center(TAC)サービスリクエストをオープンするか、サポート組織に問い合わせることをお勧めします。これらの脆弱性に対して公開されている可能性があるSMUを見つける方法の詳細については、『Cisco IOS XRソフトウェアメンテナンスアップデート(SMU)について』の「Cisco.comからのSMUのダウンロード」セクションを参照してください。

次の表では、左の列に該当するCisco IOS XRソフトウェアの機能領域を、中央の列に該当するリリースとプラットフォームを、右の列に機能領域がこの脆弱性の影響を受けるかどうかと、適切なSMUを見つけるために使用できるSMUのIDを示します。たとえば、Cisco IOS XRv 9000ルータBGP用のリリース24.2.2のSMUは、xrv9k-24.2.2.CSCwu14807.tarという名前になります。

注：SMUのIDは一意のIDであり、Cisco Bug IDではありません。 すべてのSMUがすべてのリリースとプラットフォームに適用されるとは限りません。

| 該当するCisco IOS XRソフトウェアの機能領域 | Cisco IOS XRソフトウェアリリースおよびプラットフォーム | SMU識別子 |
|---|---|---|
| すべてのXR7(LNT)プラットフォーム[1] | すべてのリリースとXR7(LNT)プラットフォーム | CSCwv19790 |
| BGP | 7.10以前のトレイン<br>26.2.1 | 脆弱性なし |
| | その他すべてのリリースおよびプラットフォーム | CSCwu14807 |
| クリプトIKE | すべてのリリースとプラットフォーム | CSCwv19170 |
| gRPC | すべてのリリースとプラットフォーム | CSCwt41683 |
| IP-SLA | すべてのリリースとプラットフォーム | CSCwv19173 |
| Intermediate System-to-Intermediate System (IS-IS) | 25.4.1 および 25.4.2 | CSCwu13271および<br>CSCwv19171[2] |
| | 26.1.2 および 26.2.1 | CSCwv19171[2] |
| | その他すべてのリリースおよびプラットフォーム | CSCwv45645および<br>CSCwv19171[2] |
| MPLS | すべてのリリースとプラットフォーム | CSCwu14825 |

| 該当するCisco IOS XRソフトウェアの機能領域 | Cisco IOS XRソフトウェアリリースおよびプラットフォーム | SMU識別子 |
|---|---|---|
| MPLS-TE | すべてのリリースとプラットフォーム | CSCwv40753[3] |
| マルチキャスト | 26.1.2 および 26.2.1 | CSCwv19180 |
| | その他すべてのリリースおよびプラットフォーム | CSCwv19180および CSCwu08799 |
| OSPF | すべてのリリースとプラットフォーム | CSCwv40741[4]および CSCwv19171[2] |
| セグメントルーティング（IPv6のみ） | 7.11.21<br>24.2.21<br>25.2.21<br>25.4.1 | CSCwv56312 |
| | 7.9.21（64ビットASR 9000シリーズアグリゲーションサービスルータ） | CSCwv56312 |
| | NCS1002上の7.3.2 | CSCwv56312 |
| | 26.1.2 および 26.2.1 | 脆弱性なし |
| | その他すべてのリリースおよびプラットフォーム | CSCwu13268[5] |
| セグメントルーティング（IPv4のみ）または セグメントルーティング（IPv4およびIPv6） | すべてのリリースとプラットフォーム | CSCwv38342 |
| TCP認証オプション | すべてのリリースとプラットフォーム | CSCwv36143[6] |
| ゼロタッチプロビジョニング(ZTP) | 26.2.1 | 脆弱性なし |
| | その他すべてのリリースおよびプラットフォーム | CSCwu36622 |

1. Cisco IOS XR7(LNT)ソフトウェアを実行するプラットフォームには、オプションの機能のインストールに関係なく、Cisco 8000シリーズルータ、Cisco NCS 1010、Cisco NCS 540Lルータ、およびCisco NCS 5700シリーズが含まれます。CLIを使用し、デバイスでCisco IOS XR7(LNT)ソフトウェアが実行されているかどうかを確認するには、このアドバイザリの「 脆弱性のある製品 」セクションを参照してください。
2. CSCwv19171は、IS-ISとOSPFの両方に適用されます。
3. CSCwv19181に代わってSMU ID CSCwv40753が使用されます。
4. SMU ID CSCwv40741がCSCwv19174に取って代わります。
5. SMU ID CSCwu13268がCSCwv19178に取って代わります。
6. SMU ID CSCwv36143がCSCwu14817に取って代わります。

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-iosxr-qg64NcM

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 1.3 | 置き換えられたSMUを更新。リリース26.1.2および26.2.1のSMUを明確化 | 修正済みリリース | Final | 2026年9月4日 |
| 1.2 | 光プラットフォームを指定し、MPLS SMUを明確にするために更新。 | 修正済みリリース | Final | 2026年9月3日 |
| 1.1 | サポート終了ソフトウェアを削除。 | 修正済みリリース | Final | 2026年9月2日 |
| 1.0 | 初回公開リリース | — | Final | 2026年9月2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。