# シスコ製品に影響するcURLおよびlibcurlの脆弱性：2023年10月


アドバイザリーID : cisco-sa-curl-libcurl-D9ds39cV
初公開日 : 2023-10-12 16:00
最終更新日 : 2024-03-05 18:03
バージョン 1.6 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID :

CVE-2023-38545

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

2023 年 10 月 11 日、cURL は、cURL ユーティリティおよび libcurl ライブラリのバージョン 8.4.0 をリリースしました。このリリースでは、次の 2 つのセキュリティに関する脆弱性が対処されています。

- CVE-2023-38545：セキュリティ影響評価（SIR）「高」
- CVE-2023-38546：SIR「低」

このアドバイザリは、CVE-2023-38545 のみを対象としています。この脆弱性の詳細については、cURL のアドバイザリを参照してください。

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-curl-libcurl-D9ds39cV

## 該当製品

シスコは製品ラインを調査して、この脆弱性により影響を受ける可能性がある製品を特定しました。

このアドバイザリは、影響を受けるソフトウェアコンポーネントを含むことが判明しており、脆弱性が存在する可能性があるシスコ製品およびサービスのみを記載しています。影響を受けるソフトウェアコンポーネントを含まない製品およびサービスは脆弱ではないため、このアドバイザリには記載されていません。このアドバイザリの「該当製品」セクションで明示されていないシスコ製品やサービスは、記載されている脆弱性の影響を受けません。

## 脆弱性のある製品

このアドバイザリの影響を受ける製品は現在確認されていません。

## 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、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

エンドポイント クライアントとクライアント ソフトウェア

- AnyConnect セキュア モビリティ クライアント

ネットワークおよびコンテンツ セキュリティ デバイス

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Firepower Threat Defense（FTD）ソフトウェア
- Identity Services Engine（ISE）
- Secure Email（旧称、E メール セキュリティ アプライアンス（ESA））
- Cisco Secure Email and Web Manager
- Cisco Secure Web Appliance

Routing and Switching - Enterprise and Service Provider

- Catalyst SD-WAN コントローラ（旧称、SD-WAN vSmart）
- Catalyst SD-WAN Manager（旧称、SD-WAN vManage）
- Catalyst SD-WAN Validator（旧称、SD-WAN vBond）
- IOS および IOS XE ソフトウェア
- IOS XR ソフトウェア
- MDS 9000 シリーズ マルチレイヤ スイッチ
- Nexus 3000 シリーズ スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- Nexus 9000 シリーズ ファブリック スイッチ（アプリケーション セントリック インフラストラクチャ（ACI）モード）
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- SD-WAN vEdge 100 シリーズ ルータ
- SD-WAN vEdge 1000 シリーズ ルータ
- SD-WAN vEdge 2000 シリーズ ルータ
- SD-WAN vEdge 5000 シリーズ ルータ

- SD-WAN vEdge Cloud ルータ

ネットワーク管理とプロビジョニング

- Application Policy Infrastructure Controller（APIC）
- Cisco Secure Network Analytics
- Telemetry Broker
- ThousandEyes Enterprise および Endpoint Agents

音声およびユニファイド コミュニケーション デバイス

- Unified Contact Center Express

Unified Computing

- HyperFlex ストレージ レプリケーション アダプタ
- HyperFlex System

## 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

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、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。

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

## 出典

この脆弱性は、2023 年 10 月 11 日に cURL のメンテナによって公開されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-curl-libcurl-D9ds39cV

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 1.6 | 脆弱性が存在しない製品のリストを更新。 | 脆弱性が存在しない製品 | Final | 2024年3月5日 |
| 1.5 | 脆弱性が存在しない製品のリストを更新。 | 脆弱性が存在しない製品 | Final | 2024 年 2 月 21 日 |
| 1.4 | アドバイザリのステータスを[Final]に変更。調査が終了したことを示すために、「該当製品」を更新。 | ヘッダー、該当製品 | Final | 2023 年 11 月 8 日 |
| 1.3 | 「調査中の製品」セクションを削除し、脆弱性が存在しないことが確認された製品のリストを更新しました。 | 該当製品 | Interim | 2023 年 10 月 31 日 |
| 1.2 | 調査中の製品のリストと脆弱性を含んでいないことが確認された製品のリストを更新。 | 該当製品 | Interim | 2023 年 10 月 20 日 |
| 1.1 | 調査中の製品のリストと脆弱性を含んでいないことが確認された製品のリストを更新。 | 該当製品 | Interim | 2023 年 10 月 13 日 |
| 1.0 | 初回公開リリース | — | Interim | 2023 年 10 月 12 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。