# Cisco Network Services Orchestratorのパストラバーサルの脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** cisco-sa-nso-path-trvsl-zjBeMkZg<br>**初公開日 :** 2023-01-11 16:00<br>**バージョン 1.0 :** Final<br>**CVSSスコア :** 5.5<br>**回避策 :** No workarounds available<br>**Cisco バグ ID :** CSCwb11065 | CVE-2023-20040 |

**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 Network Services Orchestrator(NSO)のNETCONFサービスにおける脆弱性により、認証されたリモートの攻撃者が、*root*ユーザとして動作している該当システムでサービス妨害(DoS)を引き起こす可能性があります。この脆弱性を不正利用するには、攻撃者がadminグループのメンバーである必要があります。

この脆弱性は、NETCONFを使用して該当デバイスにパッケージをアップロードする際に、ユーザ入力が適切に検証されないことに起因します。攻撃者は、この脆弱性を不正利用して、特別に巧妙に細工されたパッケージファイルをアップロードする可能性があります。エクスプロイトに成功すると、攻撃者は巧妙に細工されたファイルをファイルシステム上の任意の場所に書き込んだり、該当デバイスのファイルシステムから任意のファイルを削除したりして、DoS状態を引き起こす可能性があります。

**注：**デフォルトでは、インストール時に**—run-as-user**オプションを使用しない限り、Cisco NSOは*root*ユーザとして実行するように設定されます。

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-nso-path-trvsl-zjBeMkZg

## 該当製品

### 脆弱性のある製品

公開時点では、この脆弱性はCisco NSOに影響を及ぼしていました。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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NETCONFを実行していないCisco NSOインストールには影響を与えないことを確認しました。

## 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。

### 修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側の列に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リリースが示されています。

| Cisco NSOリリース | First Fixed Release（修正された最初のリリース） |
|---|---|
| 3.3 ~ 5.3 | 修正済みリリースに移行。 |
| 5.4 | 5.4.7 |

| | |
|---|---|
| 5.5 | 5.5.6 |
| 5.6 | 5.6.7 |
| 5.7 | 5.7.4 |
| 5.8 | 5.8.1 |
| 6.0 | 脆弱性なし |

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された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

この脆弱性は、Cisco Advanced Security Initiatives Group（ASIG）の Arthur Vidineyev による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-nso-path-trvsl-zjBeMkZg

## 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 | 2023年1月11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。