# Cisco NX-OSソフトウェアのPythonサンドボックスエスケープの脆弱性

Medium

アドバイザリーID : cisco-sa-nxos-psbe-ce-YvbTn5du
初公開日 : 2024-08-28 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCwh77779 CSCwi52383 CSCwi52460 CSCwi52362 CSCwi52461 CSCwi52363 CSCwi52380 CSCwh77781 CSCwi52365 CSCwh77780

CVE-2024-20286
CVE-2024-20285
CVE-2024-20284

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 NX-OSソフトウェアのPythonインタープリタに含まれる複数の脆弱性により、認証された権限の低いローカル攻撃者がPythonサンドボックスをエスケープして、デバイスの基盤となるオペレーティングシステムに不正アクセスする可能性があります。

この脆弱性は、ユーザ提供による入力の検証が不十分であることが原因です。攻撃者は、Pythonインタープリタ内の特定の機能を操作することで、これらの脆弱性を不正利用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Pythonサンドボックスをエスケープし、認証されたユーザの権限を使用して基盤となるオペレーティングシステムで任意のコマンドを実行できる可能性があります。

注：攻撃者がこれらの脆弱性を不正利用するには、Python実行権限で認証される必要があります。Python実行権限の詳細については、製品固有のマニュアルを参照してください。たとえば、『Cisco Nexus 9000 Series NX-OS Programmability Guide』の「Cisco NX-OS Security with Python」セクションなどです。

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-psbe-ce-YvbTn5du

このアドバイザリは、2024年8月に公開されたCisco FXOSおよびNX-OSソフトウェアセキュリティアドバイザリバンドルの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: August 2024 Semiannual Cisco FXOS and NX-OS Software Security Advisory Bundled Publication』を参照してください。

# 該当製品

## 脆弱性のある製品

公開時点で、これらの脆弱性は、Cisco NX-OSソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えました。

- MDS 9000シリーズマルチレイヤスイッチ(CSCwi52362、CSCwi52380、CSCwi52460)
- Nexus 3000シリーズスイッチ(CSCwh77779、CSCwh77780、CSCwh77781)
- Nexus 5500プラットフォームスイッチ(CSCwi52365、CSCwi52383)
- Nexus 5600プラットフォームスイッチ(CSCwi52365、CSCwi52383)
- Nexus 6000シリーズスイッチ(CSCwi52365、CSCwi52383)
- Nexus 7000シリーズスイッチ(CSCwi52363、CSCwi52461)
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCwh77779、CSCwh77780、CSCwh77781)

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。

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for VMware vSphere
- ACI モードの Nexus 9000 シリーズ ファブリック スイッチ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- UCS 6200 シリーズ ファブリック インターコネクト
- UCS 6300 シリーズ ファブリック インターコネクト
- UCS 6400 シリーズ ファブリック インターコネクト

- UCS 6500 シリーズ ファブリック インターコネクト

## 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

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。

### Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS IOS ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco Nexus 3000 シリーズ スイッチの場合は 7.0(3)I7(5)、ACI モードの Cisco NX-OS ソフトウェアの場合は 14.0(1h) です。
5. [チェック（Check）] をクリックします。

| | | |
|---|---|---|
| 2 | | Critical,High,Medium |
| このアドバイザのみ | Cisco NX-OS ソフトウェア | |
| あらゆるプラットフォーム | | |

Enter release number | Check

## Cisco Nexus 3000 および 9000 シリーズ スイッチ SMU

シスコは、Cisco NX-OSソフトウェアリリース9.3(13)に関するこれらの脆弱性に対処するために、次のSMUをリリースしました。SMUは、Cisco.comのSoftware Centerからダウンロードできます。その他の修正済みソフトウェアリリースは、前のセクションで説明したように、Cisco Software Checkerで確認できます。

| Cisco NX-OS ソフトウェアリリース | Platform | SMU 名 |
|---|---|---|
| 9.3(13) | Nexus 3000 および 9000 シリーズ スイッチ | nxos.CSCwh77779-n9k_ALL-1.0.0-9.3.13.lib32_n9000.rpm |

注：上記の表に記載されているSMUは、Cisco Nexus 3000および9000シリーズスイッチに影響する3つの脆弱性、CSCwh7779、CSCwh77780、およびCSCwh77781の修正を組み合わせたものです。

Cisco Nexus 3000および9000シリーズスイッチ用Cisco NX-OSソフトウェアでのSMUのダウンロードとインストールの詳細については、『Cisco Nexus 3000 Series NX-OS System Management Configuration Guide』および『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』の「Performing Software Maintenance Upgrades」の項を参照してください。

## 関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェアリリースの決定に際してサポートが必要な場合は、以下の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco MDS シリーズ スイッチ
VMware 向け Cisco Nexus 1000V スイッチ
Cisco Nexus 3000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 5600 プラットフォームスイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS ソフトウェアに最適なリリースを確認するには、デバイスのリリースノートに記載されている推奨リリースに関するドキュメントを参照してください。

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト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、Cisco Advanced Security Initiatives Group(ASIG)のChris Deanによる社内セキュリティテストで発見されたものです。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-psbe-ce-YvbTn5du

## 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 | 2024年8月28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。