

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



Advisory ID : cisco-sa-nxos-mppe-dhKZAFgb

[CVE-2026-20032](#)

初公開日 : 2026-10-07 16:00

バージョン 1.0 : Final

CVSSスコア : [4.4](#)

回避策 : No workarounds available

Cisco Bug ID : [CSCws98543](#) [CSCwt81529](#)
[CSCwt81528](#)

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

Cisco NX-OSソフトウェアのPythonインタープリタの脆弱性により、権限の低い認証されたローカル攻撃者が、Pythonサンドボックスをエスケープして、該当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にアクセスできる可能性があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。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ようになります。

注：この脆弱性を不正利用するには、攻撃者は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（『[Cisco Nexus 9000 Series NX-OS Programmability Guide](#)』の「Cisco NX-OS Security with Python」セクションなど）を参照してください。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-nxos-mppe-dhKZAFgb>

本アドバイザリは一連のアドバイザリの一部です。これらのアドバイザリとリンクの一覧については、[2026年10月7日発行のCisco Advance Notification, Security Advisories](#)を参照してください

。Cisco NX-OSソフトウェアの改善点と修正プログラムの詳細については、『[Cisco NX-OSソフトウェアセキュリティ強化リリース：2026年10月](#)』を参照してください。

該当製品

脆弱性がある製品

公開時点で、次のシスコ製品で脆弱性のあるCisco NX-OSソフトウェアリリースを実行していて、Python実行権限を設定された低特権ユーザが使用している場合、この脆弱性の影響を受けました。

- MDS 9000シリーズマルチレイヤスイッチ([CSCwt81528](#))
- Nexus 3000シリーズスイッチ([CSCws98543](#))
- Nexus 7000シリーズスイッチ([CSCwt81529](#))
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ([CSCws98543](#))

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[脆弱性が存在する製品](#)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。

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。

- 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
- ACIモードのNexus 9000シリーズファブリックスイッチ
- Cisco Secure Firewall 200 シリーズ
- Cisco Secure Firewall 1200 シリーズ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- Cisco Secure Firewall 6100 シリーズ
- 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
- UCS 6600 シリーズ ファブリック インターコネクト
- UCS X シリーズ ダイレクト ファブリック インターコネクト 9108 100G

回避策

この脆弱性に対処する回避策はありません。

Live Protect シールド

シスコは、Cisco NX-OSソフトウェアのこの脆弱性を一時的に緩和するために、CVE-2026-20032用の[Live Protectシールド](#)をリリースしました。このLive Protectシールドを展開すると、新しいCLIセッションのみが保護され、既存のセッションは保護されません。

Cisco NX-OS ソフトウェア用の Live Protect の詳細については、『[Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#)』を参照してください。

注：Live Protect シールドは、ソフトウェアの更新が予定されるまでの間、そのギャップを埋めるための一時的な緩和策です。この脆弱性を修正するには、このアドバイザリの「[修正済みソフトウェア](#)」セクションに記載されている修正済みソフトウェアリリースにアップグレードします。

修正済みソフトウェア

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を修正し、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。

Cisco FXOS および NX-OS ソフトウェア

お客様がCisco FXOSおよびNX-OSソフトウェアの脆弱性による侵害を判定できるように、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(例：Cisco Firepower 4100シリーズセキュリティアプライアンスの場合は2.14.1.131、Cisco Nexus 3000シリーズスイッチの場合は10.4(4))。
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 FXOSソフトウェア
あらゆるプラットフォーム		

Enter release number	Check
----------------------	-------

その他のリソース

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新しいリリースが推奨される場合、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](#)
- [Cisco Nexus 3000 シリーズ スイッチ ページ](#)
- [Cisco Nexus 7000 シリーズ スイッチ](#)
- [Cisco Nexus 9000 シリーズ スイッチ ページ](#)
- [Cisco Nexus 9000シリーズACIモードスイッチ](#)

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) 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

シスコは、この脆弱性を報告していただいたDorjsambuu Khishigdavaa氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-mppe-dhKZAFgb>

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2026年10月7日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

Cisco.com の [シスコサポート & ダウンロード](#) ページには、ライセンスとダウンロードに関する情報が記載されています。このページには、マイデバイス (My Devices) ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、[Cisco Technical Assistance Center \(TAC \)](#) に連絡してアップグレードを入手してください。無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

[ソフトウェアのアップグレードを検討する](#) 際には、関連するシスコ製品の[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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。本セキュリティアドバイザリの最新版については、[シスコ セキュリティ アドバイザリ](#) ページをご覧ください。Cisco 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評価します。詳細については、[シスコのセキュリティ脆弱性ポリシー](#)を参照してください。

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。