Cisco NX-OS ソフトウェア Python パーサー 特権 拡大脆弱性

Medium	**アドバイザリーID :** cisco-sa-20190515-nxos-pyth-escal **初公開日 :** 2019-05-15 16:00 **最終更新日 :** 2019-05-28 15:17 **バージョン 1.1 :** Final **CVSSスコア :** 4.2 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvh24788 CSCvi99282 CSCvi99284 CSCvi99288	CVE-2019-1727

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 スクリプトを書くサブシステムの脆弱性は攻撃者の特権レベルを上げる Python パーサーおよび問題任意のコマンドをエスケープする認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性は影響を受けたデバイスのスクリプトを書くサンドボックスのある特定の Python 機能に通じるユーザが指定するパラメータの不十分な sanitization が原因です。 攻撃者はスクリプトを書くサンドボックスをエスケープし、攻撃者の特権レベルを上げる任意のコマンドを実行するのにこの脆弱性を不正利用する可能性があります。

この脆弱性を不正利用するために、攻撃者は管理上または Python 実行特権の目標とされたデバイスへのローカル アクセスがあるおよび認証する必要があります。 これらの必要条件は正常なエクスプロイトの可能性を制限する可能性があります。

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ました。 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-pyth-escal

該当製品

脆弱性のある製品

本脆弱性は、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す。

- 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 3500 プラットフォーム スイッチ
- Nexus 3600 プラットフォーム 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 7700 シリーズ スイッチ
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- Nexus 9500 R シリーズ スイッチング プラットフォーム

脆弱性が存在する Cisco NX-OS 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」の項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のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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 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
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- 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）
- 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

回避策

この脆弱性に対処する回避策はありません。 ただし、管理者は非常に信頼されたユーザだけ

Python サンドボックスにアクセスすることができるようにすることによってこの脆弱性への公開を減らすことができます。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts 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完全なアップグレード ソリューション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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。

サービス契約をご利用でないお客様

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 TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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。

修正済みリリース

アップグレード アクションは行進 2019 Cisco FXOS をおよび NX-OS ソフトウェア 当たるために既に推奨されるリリースをバンドル加えてしまった顧客向けに必要ではないです。 次のシスコ

のイベント レスポンスを参照してください。 2019 年 3 月に公開された Cisco FXOS および NX-OS ソフトウェアのセキュリティ アドバイザリ バンドルの一覧

行進に 2019 のバンドルを当たるために推奨されるリリースを加えなかった顧客はこのセクションの適当な表に示すように適切なリリースにアップグレードするように勧告されます。 次の表では、左の列は Cisco NX-OS ソフトウェア リリースをリストします。 右の列は、この脆弱性が修正済みの最初の推奨リリースです。

MDS 9000 シリーズ マルチレイヤ スイッチ： CSCvi99284

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
5.2	8.1(1b)
6.2	8.1(1b)
7.3	8.1(1b)
8.1	8.1(1b)
8.2	8.3(1)
8.3	8.3(1)

スタンドアロン NX-OS モードの Nexus 3000 シリーズ スイッチ、Nexus 3500 プラットフォーム スイッチおよび Nexus 9000 シリーズ スイッチ: CSCvh24788

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
7.0(3)I4 よりも前	7.0(3)I4(8)
7.0(3)I4	7.0(3)I4(8)
7.0(3)I5	7.0(3)I7(3)
7.0(3)I6	7.0(3)I7(3)
7.0(3)I7	7.0(3)I7(3)
9.2(1)	脆弱性なし

Nexus 3600 プラットフォーム スイッチおよび Nexus 9500 R シリーズ スイッチング プラットフォーム: CSCvi99282

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
7.0(3)	7.0(3)F3(5)
9.2	脆弱性なし

Nexus 5500、5600、6000 シリーズ スイッチ： CSCvi99288

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
7.3 前	7.3(4)N1(1)
7.3	7.3(4)N1(1)

Nexus 7000 および 7700 シリーズ スイッチ CSCvi99284

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
6.2 より前	脆弱性なし

6.2	脆弱性なし
7.2	7.3(3)D1(1)
7.3	7.3(3)D1(1)
8.0	8.3(1)
8.1	8.3(1)
8.2	8.3(1)
8.3	8.3(1)

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェア リリースの決定に関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 シリーズおよび 3500 シリーズ スイッチ
Cisco Nexus 5000 シリーズ スイッチ
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 シリーズ スイッチ
Cisco Nexus 9000 シリーズ スイッチ
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS に最適な Cisco NX-OS ソフトウェア リリースの確認に関してサポートが必要な場合は、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やその公表を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-pyth-escal

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	Nexus 7000 および 7700 を修復されたリリース表更新しました。	修正済みソフトウェア	最終版	2019-May-28
1.0	初回公開リリース		最終版	2019 年 5 月 15 日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、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。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。