

# Cisco NX-OS ソフトウェア リモート パッケージ Manager コマンド インジェクト脆弱性

<b>Medium</b>	アドバイザーID : cisco-sa-20190515-nxos-rpm-injec	<a href="#">CVE-2019-1732</a>
	初公開日 : 2019-05-15 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : <a href="#">6.4</a>	
	回避策 : No workarounds available	
	Cisco バグ ID : <a href="#">CSCvi01453</a> <a href="#">CSCvj00550</a>	

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 ソフトウェアのリモート パッケージ マネージャ (RPM) サブシステムの脆弱性はタイムの使用 (TOCTOU) 競合状態管理者の資格情報が付いている任意のコマンド インジェクトの原因となる可能性があるローカル変数を破損するためにタイムのチェックにてこ入れする認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性は使用されるまで静的にとどまる必要がある重要な変数の適切な施錠機能の欠如が原因です。攻撃者は影響を受けたデバイスにによって認証し、一組の RPM 関連の CLI コマンドを発行することこの脆弱性を不正利用する可能性があります。正常なエクスプロイトは攻撃者が任意のコマンド インジェクトを行うことを可能にする可能性があります。攻撃者は目標とされたデバイスのための管理者の資格情報を必要とします。

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。

このアドバイザーは、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-rpm-injec>

## 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。

- 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
- 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
- MDS 9000 シリーズ マルチレイヤ スイッチ
- [Nexus 1000V Switch for Microsoft Hyper-V](#)
- [Nexus 1000V Switch for VMware vSphere](#)
- 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
- 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。

## 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です。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なではありません。 [Cisco イベント応答](#)が表示されて下さい: [行進 2019 Cisco FXOS および NX-OS ソフトウェア Security Advisory](#) はバンドルのアドバイザリのリストのための [パブリケーションを組み込みました](#)。

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のための修正を含む最初のリリースを示します。

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: [CSCvi01453](#)

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(9)
7.0(3)I4	7.0(3)I4(9)
7.0(3)I7	7.0(3)I7(4)
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: [CSCvj00550](#)

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

## 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ーにより新しいリリースが推奨されている場合は、そのアドバイザー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、本アドバイザー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-rpm-injec>

## 改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019-May-15

## 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、単独の転載や意識を施した場合、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。