

# Cisco NX-OS ソフトウェアの Netstack におけるサービス妨害に関する脆弱性

High

アドバイザリーID : cisco-sa-20190306-nxos-netstack

[CVE-2019-1599](#)

初公開日 : 2019-03-06 16:00

バージョン 1.0 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvm53113](#)

[CSCvm53112](#) [CSCvm53115](#)

[CSCvm53114](#) [CSCvm53125](#)

[CSCvm53128](#) [CSCvm53116](#)

[CSCvm53108](#) [CSCvk55013](#)

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 ソフトウェアのネットワーク スタックにおける脆弱性により、認証されていないリモート攻撃者が、該当デバイスでサービス妨害 (DoS) 状態を引き起こせるようになります。

この脆弱性は、ネットワーク スタックにおけるメモリ バッファの割り当てと解放の問題に起因しています。攻撃者が、持続的な方法で該当デバイスに細工された TCP ストリームを送信することにより、この脆弱性を 익스プロイトする可能性があります。 익스プロイトが成功すると、該当デバイスのネットワーク スタックにおいて使用可能なバッファが使い果たされて、コントロールプレーン プロトコルと管理プレーン プロトコルの動作が損なわれ、DoS 状態に陥ることがあります。

注: この脆弱性は、該当デバイスを宛先とするトラフィックによってのみトリガーされ、該当デバイスを通るトラフィックを使用して 익스プロイトされることはありません。

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-20190306-nxos-netstack>

このアドバイザリは、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部です。このバンドルの中には、26件の脆弱性に関する25件のシスコセキュリティアドバイザリが含まれています。これらのアドバイザリとリンクの一覧については、以下を参照してください。 [シスコのイベント対応：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](#)。

## 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 1000V Switch for Microsoft Hyper-V](#)
- [Nexus 1000V Switch for VMware vSphere](#)
- 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 ラインカードおよびファブリック モジュール
- UCS 6200 シリーズ ファブリック インターコネクト<sup>1</sup>
- UCS 6300 シリーズ ファブリック インターコネクト<sup>1</sup>
- UCS 6400 シリーズ ファブリック インターコネクト<sup>1</sup>

<sup>1</sup>UCS ファブリック インターコネクトは、影響を受けるネットワーク スタックを使用しません。ただし現在のところ、これらの製品の攻撃ベクトルは不明です。

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。

### Cisco NX-OS ソフトウェア リリースの判別

管理者は、デバイスの CLI で `show version` コマンドを使用することによって、デバイスで実行されている Cisco NX-OS ソフトウェアのリリースをチェックできます。デバイスが Cisco NX-OS ソフトウェア リリース 7.0(3)15(1) を実行している場合、コマンドの出力例は次のようになります。

```
nxos-switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
```

Copyright (C) 2002-2016, Cisco and/or its affiliates.  
All rights reserved.

The copyrights to certain works contained in this software are owned by other third parties and used and distributed under their own licenses, such as open source. This software is provided "as is," and unless otherwise stated, there is no warranty, express or implied, including but not limited to warranties of merchantability and fitness for a particular purpose. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or GNU General Public License (GPL) version 3.0 or the GNU Lesser General Public License (LGPL) Version 2.1 or Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at  
<http://www.opensource.org/licenses/gpl-2.0.php> and  
<http://opensource.org/licenses/gpl-3.0.html> and  
<http://www.opensource.org/licenses/lgpl-2.1.php> and  
<http://www.gnu.org/licenses/old-licenses/library.txt>.

Software

```
BIOS: version 07.57
NXOS: version 7.0(3)I5(1) [build 7.0(3)I5(0.9)]
BIOS compile time: 06/29/2016
NXOS image file is: bootflash:///nxos.7.0.3.I5.0.9.bin
NXOS compile time: 8/1/2016 23:00:00 [08/02/2016 00:30:32]
```

.  
.  
.

## 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 ファイアウォール
- FirePOWER 4100 シリーズ次世代ファイアウォール製品
- 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 2000 シリーズ ファブリック エクステンダ](#)
- 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 )

## 詳細

この脆弱性は、*Netstack* として知られる Cisco NX-OS ソフトウェアのネットワーク スタックにおけるバッファの割り当てと解放の問題に起因しています。該当デバイスで使用可能なバッファが使い果たされると、複数の ( ルーティング プロトコルを含む ) コントロール プレーン プロトコルと管理プロトコルがデバイスで適切に動作しなくなり、DoS 状態に陥る可能性があります。実際の影響は、デバイスで使用している特定のプラットフォームや Cisco NX-OS ソフトウェア リリースによって異なる場合があります。

この脆弱性は、該当デバイスを宛先とする TCP トラフィックによってのみトリガーされ、該当デバイスを通るトラフィックを使用してエクスプロイトされることはありません。

この脆弱性をエクスプロイトするには、攻撃者は該当デバイスの開いている TCP ポートへの TCP 接続を確立する必要があります。結果として、スプーフィングされた IP アドレスを使用して攻撃を実行することはできません。

## セキュリティ侵害の痕跡

この脆弱性がエクスプロイトされると、該当デバイスで使用可能なネットワーク スタック バッファのすべてが消費され、次のようなエラー メッセージが生成される可能性があります。

```
2019 Jan 4 11:25:00 nexus %NETSTACK-2-MPULLUP: netstack [15934] p_ip_output: m_pullup failed for IP, error ...
```

このエラー メッセージが表示される原因は複数あります。デバイスでこのメッセージが表示されたお客様については、サポート組織に連絡して、それがこの脆弱性のエクスプロイトによるデバイスの侵害を示しているのかどうかを判断してもらうことをお勧めします。

## 回避策

この脆弱性に対処する回避策はありません。

『[シスコ NX-OS ソフトウェア デバイス セキュリティ ガイド](#)』で推奨されているように、インフラストラクチャ アクセス コントロール リスト ( iACL ) と vty ACL を使用すれば、確実に信頼できる送信元 IP アドレスからのアクセスだけを許可して攻撃対象領域を縮小することが可能です。

## 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

[この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。](#) 完全なアップグレードソリューションを確認するにあたっては、このアドバイザリが、公開されたバンドルの一部であることを考慮する必要があります。バンドルアドバイザリの完全なリストは、次のページにあります。 [シスコのイベントレスポンス：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。](#)

次の表では、左の列に Cisco FXOS ソフトウェアまたは Cisco NX-OS ソフトウェアのリリースを示しています。中央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するかどうか、および、この脆弱性に対する修正を含む最初のリリースを示しています。右の列では、今回のアドバイザリバンドルに記載された脆弱性全体に対する最初の修正リリースを、影響を受けるソフトウェアリリースごとに記載しています。

各表の右の列に記載されているリリースには、脆弱性に対する修正が含まれていますが、[Cisco NX-OS ソフトウェアイメージの署名検証に関する脆弱性](#)に関連する修正については、ソフトウェアアップグレードの一部として BIOS をアップグレードする必要があります。以下に示すいずれかの製品のソフトウェアをアップグレードする場合は、このアドバイザリに記載されている BIOS アップグレードと、該当製品の ID および BIOS バージョンの詳細を参照することをお勧めします。

- Nexus 3000 シリーズ スイッチ
- ACI モードの Nexus 9000 シリーズ ファブリック 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 ラインカードおよびファブリック モジュール

Microsoft Hyper-V 向け Nexus 1000V スイッチ : [CSCvm53112](#)

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	アドバイザリバンドルに記載されている脆弱性全体に対する最初の修正リリース
5.2 より前	5.2(1)SM3(2.1)	5.2(1)SM3(2.1)
5.2	5.2(1)SM3(2.1)	5.2(1)SM3(2.1)

VMware vSphere 向け Nexus 1000V スイッチ : [CSCvm53113](#)

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	アドバイザリバンドルに記載されている脆弱性全体に対する最初の修正リリース
5.2 より前	5.2(1)SV3(4.1a)	5.2(1)SV3(4.1a)
5.2	5.2(1)SV3(4.1a)	5.2(1)SV3(4.1a)

Nexus 3000 シリーズ スイッチ : [CSCvk55013](#)

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	アドバイザリバンドルに記載されている脆弱性全体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)I7(6)
7.0(3)I4	7.0(3)I4(9)	7.0(3)I7(6)
7.0(3)I5	7.0(3)I7(6)	7.0(3)I7(6)
7.0(3)I6	7.0(3)I7(6)	7.0(3)I7(6)
7.0(3)I7	7.0(3)I7(6)	7.0(3)I7(6)
9.2	9.2(2)	9.2(2)

Nexus 3500 プラットフォーム スイッチ : [CSCvm53114](#)

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	アドバイザリバンドルに記載されている脆弱性全体に対する最初の修正リリース
6.0(2)A8 より前	6.0(2)A8(11)	6.0(2)A8(11)
6.0(2)A8	6.0(2)A8(11)	6.0(2)A8(11)
7.0(3)	7.0(3)I7(6)	7.0(3)I7(6)
9.2	9.2(2)	9.2(2)

Nexus 3600 プラットフォーム スイッチ : [CSCvm53108](#)

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	アドバイザリバンドルに記載されている脆弱性全体に対する最初の修正リリース
------------------------	--------------------	--------------------------------------

トウェア リリース		
7.0(3)	7.0(3)F3(5)	7.0(3)F3(5)
9.2	9.2(2)	9.2(2)

Nexus 5500、5600、6000 シリーズ スイッチ : [CSCvm53115](#)

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	アドバイザリ パンドルに記載されている脆弱性全体に対する最初の修正リリース
5.2 より前	7.1(5)N1(1b)	7.1(5)N1(1b)
5.2	7.1(5)N1(1b)	7.1(5)N1(1b)
6.0	7.1(5)N1(1b)	7.1(5)N1(1b)
7.0	7.1(5)N1(1b)	7.1(5)N1(1b)
7.1	7.1(5)N1(1b)	7.1(5)N1(1b)
7.2	7.3(5)N1(1)	7.3(5)N1(1)
7.3	7.3(5)N1(1)	7.3(5)N1(1)

Nexus 7000 および 7700 シリーズ スイッチ [CSCvm53128](#)

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	アドバイザリ パンドルに記載されている脆弱性全体に対する最初の修正リリース
6.2 より前	6.2(22)	6.2(22)
6.2	6.2(22)	6.2(22)
7.2	7.3(3)D1(1)	8.2(3)
7.3	7.3(3)D1(1)	8.2(3)
8.0	8.2(3)	8.2(3)
8.1	8.2(3)	8.2(3)
8.2	8.2(3)	8.2(3)
8.3	8.3(2)	8.3(2)

スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ : [CSCvk55013](#)

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	アドバイザリ パンドルに記載されている脆弱性全体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)I7(6)
7.0(3)I4	7.0(3)I4(9)	7.0(3)I7(6)
7.0(3)I5	7.0(3)I7(6)	7.0(3)I7(6)
7.0(3)I6	7.0(3)I7(6)	7.0(3)I7(6)
7.0(3)I7	7.0(3)I7(6)	7.0(3)I7(6)
9.2	9.2(2)	9.2(2)

Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール : [CSCvm53108](#)

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	アドバイザリバンドルに記載されている脆弱性全体に対する最初の修正リリース
7.0(3)	7.0(3)F3(5)	7.0(3)F3(5)
9.2	9.2(2)	9.2(2)

UCS 6200 および 6300 シリーズ ファブリック インターコネクト : [CSCvm53116](#)

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	アドバイザリバンドルに記載されている脆弱性全体に対する最初の修正リリース
3.1 より前	3.2(3j)	3.2(3j)
3.1	3.2(3j)	3.2(3j)
3.2	3.2(3j)	3.2(3j)
4.0	4.0(2a)	4.0(2a)

UCS 6400 シリーズ ファブリック インターコネクト : [CSCvm53125](#)

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	アドバイザリバンドルに記載されている脆弱性全体に対する最初の修正リリース
4.0	4.0(2a)	4.0(2a)

## 関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェア リリースの確認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स्पloit事例やその公表を確認していません。

## 出典

この脆弱性を報告していただいた Akamai 社の Tim April 氏、Trevers Astheimer 氏、Aaron Block 氏、John-Nicholas Furst 氏、および Eric Kloster 氏に感謝いたします。

## URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-netstack>

## 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 年 3 月 6 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。