# Cisco NX-OSソフトウェアのICMPバージョン6のメモリリークに関するDoS脆弱性

Medium

アドバイザリーID : cisco-sa-fxos-nxos-icmpv6-dos-YD55jVCq
CVE-2021-1229
初公開日 : 2021-02-24 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCvv96593 CSCvv96592 CSCvv24541

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ICMPバージョン6(ICMPv6)処理の脆弱性により、認証されていないリモートの攻撃者が低速のシステムメモリリークを引き起こし、それが時間の経過とともにサービス妨害(DoS)状態につながる可能性があります。

この脆弱性は、IPv6が設定されたインターフェイスが特定のタイプのICMPv6パケットを受信したときの不適切なエラー処理に起因します。攻撃者は、巧妙に細工されたICMPv6パケットを一定のレートでターゲットデバイスのローカルIPv6アドレスに送信することにより、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、攻撃者はデバイスのICMPv6プロセスでシステムメモリリークを引き起こす可能性があります。その結果、ICMPv6プロセスでシステムメモリが使い果たされ、トラフィックの処理が停止する可能性があります。その後、デバイスはすべてのICMPv6パケットをドロップし、デバイス上のトラフィックが不安定になる可能性があります。デバイスの機能を復元するには、デバイスを再起動する必要があります。

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-fxos-nxos-icmpv6-dos-YD55jVCq

## 該当製品

### 脆弱性のある製品

公開時点では、Cisco NX-OSソフトウェアの脆弱性のあるリリースを実行し、少なくとも1つのインターフェイスがIPv6トラフィック用に設定されている次のシスコ製品が、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(CSCvv24541)
- VMware vSphere向けNexus 1000 Virtual Edge(CSCvv96593)
- Microsoft Hyper-V向けNexus 1000Vスイッチ(CSCvv96593)
- VMware vSphere向けNexus 1000Vスイッチ(CSCvv96593)
- Nexus 3000シリーズスイッチ(CSCvv24541)
- Nexus 5500プラットフォームスイッチ(CSCvv24541)
- Nexus 5600プラットフォームスイッチ(CSCvv24541)
- Nexus 6000シリーズスイッチ(CSCvv24541)
- Nexus 7000シリーズスイッチ(CSCvv24541)
- 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)モードのNexus 9000シリーズファブリックスイッチ(CSCvv96592)
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCvv24541)

このアドバイザリの公開時点で脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

## Cisco NX-OS ソフトウェアの IPv6 のステータスを確認する

デバイスが着信IPv6パケットを受け入れるかどうかを確認するには、デバイスのCLIでshow ipv6 interface brief vrf allコマンドを使用します。次の例に示すように、少なくとも 1 つのインターフェイスから IPv6 インターフェイスステータスが返される場合、デバイスはこの脆弱性の影響を受ける可能性があります。

<#root>

```
Switch#

show ipv6 interface brief vrf all


IPv6 Interface Status for VRF "default"(1)
Interface         IPv6 Address/Link-local Address          Interface Status
                                                           prot/link/admin

Eth1/65           2001:db8:1:f101::1

                                up/up/up

                  fe80::23a:7dff:fe95:d071


IPv6 Interface Status for VRF "management"(2)
```

```
Interface        IPv6 Address/Link-local Address          Interface Status
                                                          prot/link/admin
```

注：Cisco NX-OSソフトウェアでは、デフォルトでIPv6アドレスは有効になっていません。Nexusデバイスのインターフェイスは、ipv6 address [...]またはipv6 link-local [...] CLIコンフィギュレーションコマンドを使用してIPv6アドレスで設定できます。また、ipv6 forward CLIコンフィギュレーションコマンドを使用すると、IPv6アドレスが設定されていない場合でも、インターフェイスでIPv6パケットを受け入れることができます。

### 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
- 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

## セキュリティ侵害の痕跡

この脆弱性により、ICMPv6プロセスでシステムメモリリークが発生します。ICMPv6メモリの枯渇により、デバイスが不安定になる可能性があります。この脆弱性が活発に不正利用された場合に発生する可能性のある侵害の兆候は、次のとおりです。

この脆弱性がデバイスで不正利用されたかどうかを判断するために追加の支援が必要な場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

### メモリの割り当て

この脆弱性がエクスプロイトされると、IPCMPv6プロセスはメモリ制限に達するまでメモリの割り当てを続行します。このメモリは返されず、回復するにはデバイスのリブートが必要です。CLIでshow processes memory sortコマンドを使用して、MemUsedフィールドを監視します。このコマンド出力には、メモリの制限も表示されます。

```
<#root>

nxos#
```

```
show processes memory sort

PID    MemAlloc  MemLimit    MemUsed     StackBase/Ptr      Process
-----  --------  ----------  ----------  -----------------  -----------
7073   561393664  1067925798  1152303104  ffc80440/ffc7fed0  icmpv6
```

show processes memory sortコマンドを使用できない場合は、CLIでshow processes memory | include icmpv6コマンドを使用します。

```
<#root>

nxos#

show processes memory | include icmpv6

PID    MemAlloc  MemLimit    MemUsed     StackBase/Ptr      Process
-----  --------  ----------  ----------  -----------------  -----------
27418  26259456  1366538124  1000681472  ffca1d60/ffca1800  icmpv6
```

### ICMPv6エラー

ICMPv6エラーに関するsyslogメッセージ（次の2つなど）を監視します。

```
<#root>

%

ICMPV6-3-ATIMERS_ERROR

: malloc failed in heap_create
```

```
<#root>

%

ICMPV6-3-ERROR

: -Traceback: librsw.so+0x11250e librs w.so+0x10be66 libam.so+0xd7f3 libam.so+0xe4cd icmpv6=0x1004
```

## 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

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 TAC もしくは契約しているメンテナンス プロバイダーまで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 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、シスコでは Cisco Software Checker を提供しています。このツールにより、特定の Cisco NX-OS ソフトウェア リリースに該当するシスコ セキュリティアドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース ( 「First Fixed」 ) を特定できます。 また該当する場合、そのリリースに関するすべてのアドバイザリ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。

お客様はCisco Software Checkerを使用して、次の方法でアドバイザリを検索できます。

- ソフトウェア、プラットフォーム、および 1 つ以上のリリースを選択する
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- show version コマンドの出力を入力する

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリまたは 1 つ以上の特定のアドバイザリが含まれるように検索をカスタマイズできます。

また、次のフォームを使用してリリースがCisco Security Advisoryのいずれかに該当するかどうかを確認し、Cisco NX-OSソフトウェアとプラットフォームを選択してリリースを入力することもできます。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。

Cisco NX-OS ソフトウェア | MDS 9000 シリーズ マルチレイヤ スイッチ

Enter Version | Check

デフォルトでは、Cisco Software Checkerには、CriticalまたはHigh Security Impact Rating(SIR)の脆弱性に関する結果のみが含まれます。 「中間」の SIR 脆弱性の結果を含めるには、Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価 ( Impact Rating ) ] ドロップダウンリストの [中間 ( Medium ) ] チェックボックスをオンにします。

## Cisco Nexus 7000 シリーズ スイッチの SMU

Cisco Nexus 7000シリーズスイッチについては、Cisco NX-OSソフトウェアリリース8.2(6)でソフトウェアメンテナンスアップグレード(SMU)を利用できます。 次の SMU を Cisco.com の Software Center からダウンロードできます。

- n7000-s2-dk9.8.2.6.CSCvx15395.bin
- n7700-s2-dk9.8.2.6.CSCvx15395.bin

Cisco Nexus 7000シリーズスイッチ用Cisco NX-OSソフトウェアでのSMUのダウンロードおよびインストールの詳細については、『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide』の「Performing Software Maintenance Upgrades」セクションを参照してください。

最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクション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 スイッチ向け Cisco Nexus 1000V
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）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

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-nxos-icmpv6-dos-YD55jVCq

## 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 | 2021 年 2 月 24 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。

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。