Cisco NX-OSソフトウェアのICMPバージョン6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 **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	CVE-2021-1229

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、その結果、サービス拒否(DoS)状態が発生す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パケットを受信する際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パケットの継続的なレートを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で、この脆弱性を不正利用する可能性があります。不正利用に成功すると、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不足し、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、デバイスがすべてのICMPv6パケットをドロップし、デバイス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-fxos-nxos-icmpv6-dos-YD55jVCq

該当製品

脆弱性のある製品

この脆弱性は、Cisco NX-OSソフトウェアの脆弱性のあるリリースを実行し、IPv6トラフィック用に少なくとも1つのインターフェイスが設定されている場合、次のシスコ製品に影響を与えました。

- MDS 9000シリーズマルチレイヤスイッチ(CSCvv24541)
- Nexus 1000 Virtual Edge for VMware vSphere(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「修正済みソフトウェア」セクションを参照して、この公開時点で脆弱性が存在していたシスコソフトウェアリリースに関する情報を確認してください。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のステータスの確認

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、コマンドが少なくとも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を返す場合、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。

```
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：デフォルトでは、Cisco NX-OSソフトウェアでは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、インターフェイスがIPv6パケットを受け入れることができるように、**ipv6 forward CLI**コンフィギュレーションコマンドを使用できます。

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。この脆弱性が積極的に悪用されている場合に発生する可能性がある侵害のインジケータを次に示します。

この脆弱性がデバイスで不正利用された可能性があるかどうかを判断するために追加のヘルプが必要な場合は、Cisco Technical Assistance Center(TAC)に連絡してください。

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継続します。このメモリは返されず、回復するにはデバイスの再起動が必要です。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**。コマンド出力には、メモリ制限も表示されます。

```
nxos# show processes memory sort
PID    MemAlloc  MemLimit    MemUsed     StackBase/Ptr      Process
-----  --------  ----------  ----------  -----------------  -----------
7073   561393664  1067925798  1152303104  ffc80440/ffc7fed0  icmpv6
```

show processes memory sortコマンドが使用できない場合は、show processes memoryコマンドを使用**してください | include icmpv6**コマンドを使用します。

```
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メッセージを監視します。次の2つのメッセージが表示されます。

- `%ICMPV6-3-ATIMERS_ERROR: malloc failed in heap_create`
- `%ICMPV6-3-ERROR: -Traceback: librsw.so+0x11250e librs w.so+0x10be66 libam.so+0xd7f3 libam.so+0xe4cd icmpv6=0x1004f000 0x100ed1b9 0x101 05623 0x10078fe7 libipv6.so+0x14988 librsw.so+0xc8658 libpthread.so.0+0x609b lib c.so.6+0xd6a5e`

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 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、すべてのアドバイザリに記載された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。

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、Cisco NX-OS ソフトウェアとプラットフォームを選択、およびリリースを入力することで（例：Cisco Nexus 3000 シリーズ スイッチの **7.0(3)I7(5)**、**ACI モードの Cisco NX-OS ソフトウェアの 14.0(1h)**）、**シスコ セキュリティ アドバイザリの対象となる**

リリースであるかを判断することもできます。

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating (SIR) が「重大」または「高」の脆弱性だけが含まれます。 「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シリーズスイッチでは、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 スイッチ向け Cisco NX-OS ソフトウェアにおける SMU のダウンロードと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」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）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-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	Date
1.0	初回公開リリース	—	最終版	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。