Cisco IOS XRソフトウェアのUDPパケットメモリ枯渇の脆弱性

High

アドバイザリーID : cisco-sa-pak-mem-exhst-3ke9FeFy
初公開日 : 2024-09-11 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 : CSCwk63828

CVE-2024-20304

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 IOS XRソフトウェアのマルチキャストトレースルートバージョン2(Mtrace2)機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスのUDPパケットメモリを枯渇させる可能性があります。

この脆弱性は、Mtrace2コードがパケットメモリを適切に処理していないことに起因しています。攻撃者は、細工を施したパケットを該当デバイスに送信することで、この脆弱性をエクスプロイトできる可能性があります。エクスプロイトに成功すると、攻撃者は着信UDPパケットメモリを枯渇させることができます。該当するデバイスでは、高レベルのUDPベースのプロトコルパケットを処理できず、サービス妨害(DoS)状態を引き起こす可能性があります。

注：この脆弱性は、IPv4またはIPv6を使用して不正利用できます。

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-pak-mem-exhst-3ke9FeFy

このアドバイザリは、2024年9月に公開されたCisco IOS XRソフトウェアセキュリティアドバイザリバンドルの一部です。アドバイザリとリンクの一覧については、Cisco Event Response: September 2024 Semiannual Cisco IOS XR Software Security Advisory Bundled Publication を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOS XRソフトウェアの脆弱性が存在するリリースを実行し、Mtrace2パケットを処理しているシスコデバイスに影響を与えます。

リリース7.7.1よりも前のCisco IOS XRソフトウェアリリースは影響を受けません。

Cisco IOS XRソフトウェアリリース7.7.1 ~ 7.11.2は、マルチキャスト設定に関係なく、マルチキャストRPM Packet Manager(RPM)がデバイスにインストールされ、アクティブになっている場合に影響を受けます。

マルチキャストRPMがインストールされてアクティブであり、デバイスにマルチキャスト設定がある場合、Cisco IOS XRソフトウェアリリース24.1.1以降が影響を受けます。マルチキャストが設定されていない場合、デバイスには脆弱性が存在しません。

脆弱性が存在する Cisco 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。

マルチキャストRPMがアクティブかどうかの確認

マルチキャストRPMがアクティブかどうかを確認するには、show install active summary | include mcastコマンドを使用します。このコマンドで空の出力が返された場合、マルチキャストRPMはアクティブではありません。

Mtrace2の処理が有効になっているかどうかの確認

デバイスがMtrace2パケットを処理しているかどうかを確認するには、show lpts pifib hardware entry brief location <LC> | include 33433コマンドとshow lpts pifib entry brief | include 33433コマンドを使用して、Mtrace2ポートに対してLPTSエントリが作成されているかどうかを確認できます。両方のコマンドが空の出力を返す場合、デバイスはMtrace2パケットを処理していません。

次の例では、デバイスはLPTSエントリを作成し、Mtrace2パケットを処理します。

RP/0/RP0/CPU0:Router#show lpts pifib hardware entry brief location 0/0/CPU0 | 33433の追加										
IPV4任意	任意	任意	0	17	33433	0	0	UDPリッスン	Dlvr RP0	LOW
IPV4任意	任意	任意	0	17	33433	0	1	UDPリッスン	Dlvr RP0	LOW
IPV4任意	任意	任意	0	17	33433	0	2	UDPリッスン	Dlvr RP0	LOW
IPV4任意	任意	任意	0	17	33433	0	0	UDPリッスン	Dlvr RP0	LOW

IPV4任意	任意	任意	0	17	33433	0	1	UDPリッスン	Dlvr RP0	LOW
IPV4任意	任意	任意	0	17	33433	0	2	UDPリッスン	Dlvr RP0	LOW
RP/0/RP0/CPU0：ルータ#										

```
RP/0/RP0/CPU0:Router# show lpts pifib entry brief | include 33433
IPv4       default  UDP    any          0/RP0/CPU0                  any,33433 any
IPv6       default  UDP    any          0/RP0/CPU0                  any,33433 any
```

注：Cisco IOS XRソフトウェアのMtrace2は、標準のRFCポート33435ではなく、非標準ポート33433を使用します。

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記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

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。

- IOS ソフトウェア
- IOS XE ソフトウェア
- NX-OS ソフトウェア

詳細

show packet memoryコマンドを使用すると、パケットメモリに現在保持されているパケットの数を確認できます。次に例を示します。

```
RP/0/RP0/CPU0:#show packet-memory summary
 ProcId JobId Count Percentage Process
   4916   328     9      0.18% tcp
   4512  1241  1125     22.46% igmp
   4527  1246  3875     77.36% mld
```

通常の動作中は、パケットカウントは低くなります。mldプロセスまたはigmpプロセスのパケット数が、コマンドを複数回実行しても着実に増加する、または減少しない場合、デバイスはこの脆弱性の影響を受けます。

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、この脆弱性に対しては緩和策があります。

Cisco IOS XRリリース7.7 ~ 7.11でRPMを非アクティブにする

デバイスでマルチキャスト設定が必要ない場合は、マルチキャストRPMを非アクティブ化して削除します。これにより、脆弱なUDPポートが閉じられます。

次の例では、マルチキャストパッケージasr9k-mcast-x64-2.0.0.0-r7921.x86_64.rpmが非アクティブ化されています。

```
Router# show install active summary | include mcast

asr9k-mcast-x64-2.0.0.0-r7921.x86_64.rpm

Router# install deactivate asr9k-mcast-x64-2.0.0.0-r7921.x86_64.rpm synchronous

Router# install commit
```

インフラストラクチャアクセスコントロールリスト(iACL)を使用したポート33433のブロック

インフラストラクチャデバイスを保護し、インフラストラクチャに対する直接攻撃のリスク、影響、および効果を最小限に抑えるために、iACLを導入して、インフラストラクチャ機器に送信されるトラフィックにポリシーを適用することが推奨されています。管理者は、既存のセキュリティポリシーと設定に従って、インフラストラクチャデバイスに送信される許可されたトラフィックのみを明示的に許可することで、iACLを構築できます。インフラストラクチャ デバイスの保護を最大にするには、IP アドレスが設定されているすべてのインターフェイスの入力方向で配備済みの iACL を適用する必要があります。信頼できる送信元アドレスから攻撃が発信されている場合、iACLの対応策ではこの脆弱性を完全に防ぐことはできません。

iACLポリシーは、該当するデバイスのUDPポート33433に送信される不正なMtrace2通信パケットを拒否します。次の例では、192.168.60.0/24が該当デバイスによって使用されるIPアドレス空間です。不正なトラフィックをすべて拒否する前に、ルーティングや管理アクセスに必要なトラフィックを許可するように注意する必要があります。インフラストラクチャのアドレス空間は、可能な限り、ユーザおよびサービスセグメントのアドレス空間とは別にする必要があります。このようにアドレスを設定することで、iACL の構築と配備が容易になります。

注:Mtrace2もIPv6をサポートしているため、デバイスにIPv6が設定されている場合は、対応するIPv6 iACLが必要です。

注：シスコでは、Mtrace2に33435ではなくUDPポート33433を使用しています。

```
ipv4 access-list Infrastructure-ACL-Policy
!
!-- The following vulnerability-specific access control entries
!-- (ACEs) can drop Mtrace version 2 communication packets
!  deny udp any 192.168.60.0 0.0.0.255 eq 33433
!
!-- Explicit deny ACE for traffic sent to addresses configured
!-- within the infrastructure address space
!  deny ip any 192.168.60.0 0.0.0.255
!
!-- Permit or deny all other Layer 3 and Layer 4 traffic in
!-- accordance with existing security policies and configurations
!
!-- Apply iACL to interfaces in the ingress direction
!
interface GigabitEthernet0/0 ipv4 access-group Infrastructure-ACL-Policy in
```

iACLについての詳細は、『コアの保護：インフラストラクチャ保護ACL』を参照してください。

IGMPおよびMLDプロセスの再起動

デバイスがメモリを使い果たす前に、Internet Group Management Protocol (IGMP)プロセスかマルチキャストリスナー検出(MLD)プロセス、あるいはその両方を再起動すれば、他のプロセスに影響を与えることはありません。（詳細については、「詳細」セクションを参照してください）。これらのプロセスを再起動しても、デバイスのUDPメモリのリークは防止されません。

process restart mldコマンドかprocess restart igmpコマンドを使用して、それぞれのプロセスを再起動します。

これらの緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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リリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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、アクセスまたはその他の方法で使用した場合、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。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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

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

次の表では、左の列にシスコソフトウェアリリースまたはトレインを示します。右の列は、リリース（トレイン）がこのアドバイザリに記載された脆弱性の影響を受けるかどうか、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。

Cisco IOS XR ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
7.6 以前	影響なし。
7.7 ~ 7.10	修正済みリリースに移行。
7.11	7.11.21（2024年10月）
24.1	修正済みリリースに移行。
24.2	24.2.2（2024年9月）

Cisco IOS XR ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
24.3.1 以降	影響なし。

シスコはこの脆弱性に対処するため、次の包括SMUをリリースしました。次の表に記載されていないリリースでSMUを必要とするお客様は、サポート組織に連絡することをお勧めします。

Cisco IOS XR ソフトウェア リリース	Platform	SMU 名
7.7.2	IOSXRWBD	iosxrwbd-7.7.2.CSCwm05729
7.11.2	IOSXRWBD NCS5500	iosxrwbd-7.11.2.CSCwm05729 ncs5500-7.11.2.CSCwm05729
24.1.2	8000 シリーズ	8000-24.1.2.CSCwm05729

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pak-mem-exhst-3ke9FeFy

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	2024年9月11日

利用規約

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。