ACI モードの Cisco Nexus 9000 シリーズ ファブリック スイッチで確認された Link Layer Discovery Protocol（LLDP）のメモリリークサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-aci-lldp-dos-ySCNZOpX

初公開日 : 2023-02-22 16:00

バージョン 1.0 : Final

CVSSスコア : 7.4

回避策 : No workarounds available

Cisco バグ ID : CSCwc23246

CVE-2023-20089

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

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Cisco Nexus 9000シリーズファブリックスイッチのLink Layer Discovery Protocol(LLDP)機能の脆弱性により、認証されていない隣接する攻撃者がメモリリークを引き起こし、デバイスの予期しないリロードが発生する可能性があります。

この脆弱性は、入力LLDPパケットを解析する際の誤ったエラーチェックに起因します。攻撃者は、巧妙に細工されたLLDPパケットの安定したストリームを該当デバイ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。エクスプロイトに成功すると、攻撃者はメモリリークを引き起こし、デバイスが予期せずリロードされたときにサービス拒否(DoS)状態を引き起こす可能性があります。

注：この脆弱性は、デバイスを通過するトランジットトラフィックによって不正利用されることはありません。巧妙に細工されたLLDPパケットは、直接接続されたインターフェイスをターゲットとする必要があり、攻撃者は該当デバイス（レイヤ2隣接）と同じブロードキャストドメインに存在する必要があります。また、この脆弱性に対する攻撃対象は、必要でないインターフェイスでLLDPを無効にすることで減らすことができます。

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-aci-lldp-dos-ySCNZOpX

このアドバイザリは、2023 年 2 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。アドバイザリの完全なリストとそのリンクについては、『Cisco Event Response: February 2023 Semiannual Cisco FXOS and NX-OS 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、ACIモードのCisco Nexus 9000シリーズファブリックスイッチでCisco NX-OSソフトウェアの脆弱性が存在するリリースを実行しており、LLDP機能が有効になっている場合に影響を与えます。

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。

LLDPが有効になっているかどうかの確認

ACIモードのCisco Nexus 9000シリーズファブリックスイッチのLLDPステータスを確認するには、**show lldp interface ethernet *port/interface***コマンドを使用します。送信(**tx**)と受信(**rx**)のステータスが**Y**の場合、次の例に示すように、インターフェイスでLLDPが有効になります。

```
#show lldp interface ethernet port/interface
Interface Information:Enable (tx/rx/dcbx): Y/Y/N    Port Mac address: 00:fe:c8:09:e2:92
```

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。

- 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
- MDS 9000 シリーズ マルチレイヤ スイッチ
- VMware vSphere 向け Nexus 1000 Virtual Edge

- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 3000 シリーズ 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
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- Cisco Secure Firewall 3100 シリーズ
- 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
- UCS 6500 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

この脆弱性のエクスプロイトにより、LLDP プロセスでメモリリークが発生する可能性があり、利用可能なシステムメモリが不足すると、デバイスがクラッシュする可能性があります。

LLDP プロセスのメモリ使用量を監視するには、CLI コマンドの **ps aux --sort -rss** または **ps aux --sort -rss | grep lldp** を使用します。出力の **VSZ** 列は、LLDP プロセスによって使用されているメモリの合計量を示しています。この数値が時間の経過とともにゆっくりと増加し、決して減少しない場合は、この脆弱性がエクスプロイトされていることを示している可能性があります。メモリを再利用するには、デバイスを再起動する必要があります。

```
leaf# ps aux --sort -rss
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root     24764  2.1  3.3 2454992 544656 ?      Ssl  Jan29 3772:19 /isan/bin/coop
root     24769  0.8  2.8 2150308 458840 ?      Ssl  Jan29 1497:31 /isan/bin/routing-sw/isis -t
isis_infra
root     22160  0.0  2.8 1966352 454464 ?      Ssl  Jan29  71:52 /isan/bin/nfm
root     56391  0.0  2.7 1963948 451276 ?      Ss   Jan29   5:49 /isan/bin/cts -t
root     24763  0.0  2.4 1918348 394152 ?      Ssl  Jan29   6:27 /isan/bin/dhcp_snoop
root     22222  0.0  2.3 1111704 379436 ?      Ssl  Jan29  67:56 /isan/bin/acllog
root     24754  0.0  2.3 1895068 378796 ?      Ss   Jan29  52:41 /isan/bin/oam
root     24757  0.0  2.3 4190440 376808 ?      Ss   Jan29 134:20 /isan/bin/lldp

leaf#ps aux --sort -rss | grep lldp
root     24757  0.0  2.3 4190440 376808 ?      Ss   Jan29 134:20 /isan/bin/lldp
```

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、インターフェイスで LLDP が有効になっていない場合は、この脆弱性をそのインターフェイスでエクスプロイトできません。リスクを緩和するために、LLDP が不要なすべてのインターフェイスで LLDP を無効にしてください。CLI コマンドの **no lldp transmit** および **no lldp**

receive を使用してください。詳細については、『Cisco APIC Layer 2 Networking Configuration Guide』を参照してください。

こ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。

Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS IOS 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に、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載の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。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。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。
5. [チェック（Check）] をクリックします。

その他のリソース

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 向け Cisco Nexus 1000V スイッチ

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

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-aci-lldp-dos-ySCNZOpX

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	2023 年 2 月 22 日

利用規約

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。