# Cisco IOSおよびIOS XEソフトウェアのレイヤ2 Traceroutesサーバの保護

Informational

アドバイザリーID : cisco-sa-20190925-l2-traceroute
初公開日 : 2019-09-25 16:00
バージョン 1.0 : Final
回避策 : No workarounds available
Cisco バグ ID :

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

レイヤ2(L2)のtracerouteユーティリティは、パケットが送信元デバイスから宛先デバイスまでとるL2パスを識別します。Cisco Catalystスイッチ用のCisco IOSソフトウェアおよびCisco IOS XEソフトウェアは、Cisco CatOSソフトウェアからL2 traceroute機能を継承しています。そのため、この機能はCisco IOSおよびIOS XEソフトウェアが最初にリリースされてからサポートされています。シスコは、L2 traceroute機能がCisco IOS XRソフトウェアまたはCisco NX-OSソフトウェアでサポートされていないことを確認しました。

Cisco CatalystスイッチのCisco IOSおよびIOS XEソフトウェアでは、L2 traceroute機能はデフォルトで有効になっています。この機能を有効にすると、IPv4を介して到達可能なL2 tracerouteサーバが起動し、UDPポート2228でリッスンします。次の例は、L2 traceroute機能が有効になっているデバイスでのshow ip socketsコマンドの出力を示しています。

```
<#root>

Switch#

show ip sockets

Proto         Remote      Port      Local       Port  In Out  Stat TTY OutputIF

17

0.0.0.0

              0 10.10.10.1

2228

   0    0    211    0
```

設計上、L2 tracerouteサーバは認証を必要とせず、影響を受けるデバイスに関する次のような特定の情報を読み取ることができます。

- ホスト名
- ハードウェアモデル
- 設定されたインターフェイス
- 設定されたIPアドレス
- VLAN データベース
- MACアドレステーブル
- レイヤ2フィルタリングテーブル
- Cisco Discovery Protocol(CDP)ネイバー情報

ネットワーク内の複数のスイッチからこの情報を読み取ることで、攻撃者はそのネットワークの完全なL2トポロジマップを構築できる可能性があります。

このアドバイザリの「推奨事項」セクションの説明に従って、L2 tracerouteサーバを保護することをお勧めします。

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-20190925-l2-traceroute

# 推奨事項

## レイヤ2 Tracerouteサーバの保護

環境内でL2 traceroute機能が使用されているかどうか、およびCisco IOSまたはIOS XEソフトウェアリリースがそれぞれのオプションを実装するCLIコマンドをサポートしているかどうかによって、L2 tracerouteサーバを保護する方法はいくつかあります。

- L2 tracerouteサーバをディセーブルにします。
- インフラストラクチャアクセスコントロールリスト(iACL)を使用して、L2 tracerouteサーバへのアクセスを制限します。
- コントロールプレーンポリシング(CoPP)により、L2 tracerouteサーバへのアクセスを制限します。
- L2 tracerouteサーバがデフォルトで無効になっているリリースにアップグレードします。

### レイヤ2 Tracerouteサーバのディセーブル化

このコマンドをサポートするCisco IOSおよびIOS XEソフトウェアリリースでは、グローバルコンフィギュレーションモードでno l2 tracerouteコマンドを使用することにより、L2 tracerouteサーバを無効にできます。no l2 tracerouteコマンドを使用できる場合は、L2 tracerouteサーバをただちに停止します。Cisco IOSまたはIOS XEソフトウェアの最近のリリースを実行していて、no

l2 tracerouteコマンドを使用できないお客様は、サポート組織に問い合わせることをお勧めします。

インフラストラクチャアクセスコントロールリストを使用したL2 Traceroute サーバへのアクセス制限

ネットワークを通過するトラフィックをブロックすることは困難ですが、悪意のあるトラフィックを特定し、そのトラフィックをネットワークの境界でブロックすることは可能です。iACLの使用はネットワークセキュリティのベストプラクティスであり、ここでの特定の問題の緩和に加えて、優れたネットワークセキュリティへの長期的な付加機能として考慮する必要があります。インフラストラクチャ IP アドレス範囲内の IP アドレスを持つすべてのデバイスを保護するには、展開された iACL の一部に次の iACL の例を含めることをお勧めします。

```
!---
!--- Feature: L2 Traceroute
!---

!---
!--- Deny L2 Traceroute traffic from all other sources
!--- destined to infrastructure addresses
!---

access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 2228

!---
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.
!---

access-list 150 permit ip any any

!---
!--- Apply access-list to all interfaces (only one example
!--- shown)
!---

interface GigabitEthernet 2/0
 ip access-group 150 in
```

iACLの導入テクニックに関する詳細なガイドラインと推奨事項については、ホワイトペーパー『コアの保護：インフラストラクチャ保護ACL』および『Cisco IOSデバイスのセキュリティ強化ガイド』を参照してください。

コントロールプレーンポリシングを使用したL2 Traceroute サーバへのアクセス制限

CoPPは、デバイスへの信頼できないUDPトラフィックをブロックするために使用できます。

CoPP機能は、Cisco IOSソフトウェアリリース12.0S、12.2SX、12.2S、12.3T、12.4、12.4T以降でサポートされています。CoPPは、次の操作を実行するように設定できます。

- 管理プレーンとコントロールプレーンの保護
- インフラストラクチャへの直接攻撃のリスクと効果を最小限に抑える

これは、既存のセキュリティポリシーと設定に従って、許可されたトラフィックだけを明示的に許可することで行われます。

インフラストラクチャIPアドレスの範囲内にあるIPアドレスを持つすべてのデバイスを保護するために、次のCoPPを、導入されたCoPPポリシーの一部として含めることを推奨します。

```
!---
!--- Feature: L2 Traceroute
!---

!---
!--- Deny L2 Traceroute traffic from all other sources
!--- destined to the device control plane.
!---

access-list 150 permit udp any any eq 2228

!---
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
!---

class-map match-all drop-l2trace-class
 match access-group 150

!---
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!---

policy-map control-plane-policy
 class drop-l2trace-class
  drop

!---
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
!---

control-plane
 service-policy input control-plane-policy
```

CoPP機能の設定と使用の詳細については、『コントロールプレーンポリシング(CoPP)の実装の

ベストプラクティス』および『Cisco IOSデバイスのセキュリティ強化ガイド』を参照してください。

デフォルトでL2 Traceroutesサーバが無効になっているリリースへのアップグレード

次に示すCisco IOSおよびIOS XEソフトウェアの計画済みリリースでは、L2 traceroutesサーバがデフォルトで無効になります。

- Cisco IOS 15.2(7)E1（2019年12月）以降
- Cisco IOS XE 3.11.1E（2019年12月）以降
- Cisco IOS XE 17.2.1（2020年3月）以降

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team(PSIRT)は、このアドバイザリに記載されているL2 traceroute機能を悪用するために使用される可能性がある公開悪用コードが存在することを認識しています。

## 出典

シスコは、この問題を報告していただいた独立したセキュリティ研究者であるChris Marget氏に感謝いたします。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-l2-traceroute

## 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 | 2019 年 9 月 25 日 |

## 利用規約

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。