Cisco Nexus 9000 シリーズ ファブリック スイッチ ACI モード ファブリック インフラストラクチャ VLAN の不正アクセスにおける脆弱性

High

アドバイザリーID : cisco-sa-20190703-n9kaci-bypass

初公開日 : 2019-07-03 16:00

バージョン 1.0 : Final

CVSSスコア : 7.4

回避策 : Yes

Cisco バグ ID : CSCvp64280

CVE-2019-1890

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 Nexus 9000 シリーズ 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 スイッチ ソフトウェアのファブリック インフラストラクチャ VLAN 接続確立における脆弱性により、認証されていない隣接する攻撃者がセキュリティ検証をバイパスし、認証されていないサーバをインフラストラクチャ VLAN に接続できるようになります。

この脆弱性は、インフラストラクチャ VLAN の Link Layer Discovery Protocol（LLDP）セットアップ段階でのセキュリティ要件が不十分であることに起因します。 攻撃者は、隣接するサブネット上で悪意のある LLDP パケットを ACI モードの Cisco Nexus 9000 シリーズ スイッチに送信することで、この脆弱性をエクスプロイトする可能性があります。 攻撃者は、エクスプロイトに成功すると、認証されていないサーバをインフラストラクチャ VLAN に接続できるようになります。 攻撃者はインフラストラクチャ VLAN への接続を使用して、Cisco Application Policy Infrastructure Controller（APIC）サービスへの不正な接続を確立したり、他のホスト エンドポイントに参加する可能性があります。

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。 本脆弱性に対処する回避策がいくつかあります。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass

該当製品

脆弱性のある製品

この脆弱性は、14.1(2g) より以前の Cisco Nexus 9000 シリーズ ACI モード スイッチ ソフトウェア リリースを実行しており、ファブリック セキュア モードのデフォルトの許可モード設定を使用している場合、ACI モードの Cisco Nexus 9000シリーズ ファブリック スイッチに影響します。 詳細については、「回避策」のセクションを参照してください。

修正済みソフトウェア 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」のセクションを参照してください。

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

シスコでは、この脆弱性が Cisco FXOS または Cisco NX-OS ソフトウェアを実行している場合、次のシスコ製品には影響を及ぼさないことを確認しています。

- 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
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 3000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- Nexus 3600 プラットフォーム 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
- Nexus 7700 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
- Nexus 9500 R シリーズ スイッチング プラットフォーム
- 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

回避策

ストリクト モードが設定されている場合、この脆弱性はエクスプロイトできません。 ストリクト モードでは、接続を許可する前に、次のファームウェア セキュリティ チェックが適用されます。

- 有効なシスコのシリアル番号とセキュア ソケット レイヤ（SSL）証明書を持つスイッチのみを許可します。
- シリアル番号ベースの認証が必要です。
- 管理者がファブリックに参加するために手動でコントローラとスイッチを承認する必要があります。

管理者は、**システム ファブリック セキュリティ モード** コマンドが実行コンフィギュレーションに存在することを確認することで、インターフェイスがストリクト モードで設定されているかどうかを判断できます。

```
apic# show running-config | grep strict
 system fabric-security-mode strict
```

ストリクト モードの設定の詳細については、「ファブリック セキュア モードの設定」を参照してください。

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts 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 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 に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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

この脆弱性は、ACI モードの Cisco Nexus 9000 シリーズ スイッチ ソフトウェア リリース 14.1(2g) 以降で修正されています。

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

この脆弱性を報告していただいた、ERNW Research 社と協力関係にある ERNW Enno Rey Netzwerke 社の Oliver Matula 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass

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	2019 年 7 月 3 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。