Cisco Nexus 3000および9000シリーズスイッチのポートチャネルACLプログラミングの脆弱性

Medium

アドバイザリーID : cisco-sa-nxos-po-acl-TkyePgvL
初公開日 : 2024-02-28 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwf47127

CVE-2024-20291

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

スタンドアロンNX-OSモードのCisco Nexus 3000および9000シリーズスイッチのポートチャネルサブインターフェイスに対するアクセスコントロールリスト(ACL)プログラミングの脆弱性により、認証されていないリモートの攻撃者が、該当デバイスを介してブロックされる必要のあるトラフィックを送信できる可能性があります。

この脆弱性は、ポートチャネルメンバーポートの設定が変更されたときに発生する誤ったハードウェアプログラミングに起因します。攻撃者は、該当デバイスを介してトラフィックを送信しようとすることで、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、攻撃者はポートチャネルサブインターフェイスに適用されたACLによって保護される必要があるネットワークリソースにアクセスでき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ています。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-po-acl-TkyePgvL

このアドバイザリは、2024年2月に公開されたCisco FXOSおよびNX-OS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: February 2024 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

公開時点では、この脆弱性は、Cisco NX-OSソフトウェアリリース9.3(10)、9.3(11)、または9.3(12)を実行していて、少なくとも1つのポートチャネルサブインターフェイスに入力ACLが設定されているスタンドアロンNX-OSモードのCisco Nexus 3000および9000シリーズスイッチに影響を与えました。次に例を示します。

```
<#root>

nxos#

show running-config interface port-channel

10.10

interface port-channel10.10
  encapsulation dot1q 10


ip access-group

 acl-10

in


  ip address 10.10.1.1/24
  no shutdown
```

注：影響を受ける設定を使用している場合、ポートチャネルメンバーポートに対して行われた変更により、ACLプログラミングエラーが発生する可能性があります。

ACLプログラミングが影響を受けるかどうかの判別

ACLプログラミングが影響を受けるかどうかを判断するには、デバイスのCLIでshow system internal access-list interface port-channel subinterface input entries detailコマンドを使用します。通常のACLプログラミング状況では、次の例に示すように、このコマンドは対象のサブインターフェイスに関連付けられたACL エントリを返すことが想定されます。

```
<#root>

nxos#

show system internal access-list interface port-channel

10.10

 input entries detail


slot  1
=======
```

```
Flags: F - Fragment entry  E - Port Expansion
       D - DSCP Expansion  M - ACL Expansion
       T - Cross Feature Merge Expansion
       N - NS Transit  B - BCM Expansion  C - COPP

INSTANCE 0x0
---------------
  Tcam 1 resource usage:
  ----------------------
  LBL B = 0xa
   Bank 1
   ------
     IPv4 Class
       Policies: RACL(acl-10)
       Netflow profile: 0
       Netflow deny profile: 0


 Entries

:
         [Index] Entry [Stats]
         ---------------------


 [0x001c:0x001e:0x001e] permit ip 0.0.0.0/0 10.10.1.11/32  routeable 0x1  [0]
  [0x001d:0x001f:0x001f] deny ip 0.0.0.0/0 10.10.1.12/32  routeable 0x1  [0]
  [0x001e:0x0020:0x0020] deny ip 0.0.0.0/0 0.0.0.0/0  routeable 0x1  [0]
```

アクセスリストを使用して設定されたポートチャネルサブインターフェイスに対してコマンドを実行してもエントリが返されない場合、次の例に示すように、ACLプログラミングが影響を受けます。

```
<#root>

nxos#

show system internal access-list interface port-channel

 10.10

input entries detail


slot  1
=======
```

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 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
- ACI モードの Nexus 9000 シリーズ ファブリック スイッチ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 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

回避策

本脆弱性に対処する回避策がいくつかあります。

ポートチャネルメンバーポートの設定を変更した後、このアドバイザリの「脆弱性のある製品」セクションで説明されているように、ACLプログラミングがポートチャネルサブインターフェイスに影響を与えているかどうかを確認します。該当するポートチャネルサブインターフェイスで適切なACLプログラミングを復元するには、関連するip access-group設定コマンドを削除して再適用します。影響を受けるデバイスをリロードすると、影響を受けるすべてのサブインターフェイスのACLプログラミングも修正されます。

これらの回避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

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。

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。

2		Critical,High,Medium
このアドバイザのみ	Cisco NX-OS ソフトウェア	
あらゆるプラットフォーム		
Enter release number	Check	

Cisco Nexus 3000 および 9000 シリーズ スイッチ SMU

シスコはこの脆弱性に対処するため、次のSMUをリリースしました。SMUは、Cisco.comのSoftware Centerからダウンロードできます。

Cisco NX-OS ソフトウェアリリース	Platform	SMU 名
9.3(12)	Nexus 3000 および 9000 シリーズ スイッチ	nxos.CSCwf47127-n9k_ALL-1.0.0-9.3.12.lib32_n9000.rpm

Cisco Nexus 3000および9000シリーズスイッチ用Cisco NX-OSソフトウェアでの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 3000シリーズスイッチ』および『Cisco Nexus 9000シリーズスイッチ』の『Cisco NX-OSシステム管理設定ガイド』の「ソフトウェアメンテナンスアップグレードの実行」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 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

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-po-acl-TkyePgvL

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2月28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。