ACIモードのCisco Nexus 9000シリーズファブリックスイッチにおけるSNMPのDoS脆弱性

High

アドバイザリーID : cisco-sa-nxos-dsnmp-cNN39Uh
初公開日 : 2026-02-25 16:00
バージョン 1.0 : Final
CVSSスコア : 7.7
回避策 : Yes
Cisco バグ ID : CSCwq57598

CVE-2026-20048

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

ACIモードのCisco Nexus 9000シリーズファブリックスイッチのSimple Network Management Protocol(SNMP)サブシステムの脆弱性により、認証されたリモートの攻撃者が該当デバイスにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、SNMP要求を解析する際の不適切な処理に起因します。攻撃者は、影響を受けるデバイスの特定のMIBにSNMPクエリを継続的に送信することにより、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、攻撃者がデバイスでカーネルパニックを引き起こし、リロードとDoS状態が発生する可能性があります。

注：この脆弱性は、SNMPバージョン1、2c、および3に影響します。SNMPv1またはSNMPv2cを介してこの脆弱性をエクスプロイトするには、攻撃者が該当システムの有効な読み取り専用SNMPコミュニティストリングを持っている必要があります。SNMPv3 でこの脆弱性をエクスプロイトするには、攻撃者は該当するシステムの有効な SNMP ユーザーログイン情報を入手している必要があります。

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-dsnmp-cNN39Uh

このアドバイザリは、2026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 2026 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、次の両方の条件を満たす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を与えます。

- SNMP機能が有効になっている。
- 少なくとも1つの認証、承認、アカウンティング(AAA)プロバイダーが、IPv4アドレスではなく、DNS名(ホスト名または完全修飾ドメイン名(FQDN))またはIPv6アドレスで構成されています。

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。

SNMP 設定の確認

特定のデバイスでSNMPv1、SNMPv2c、またはSNMPv3が有効になっているかどうかを確認するには、次の例に示すように、スイッチのCLIからshow snmp summary CLIコマンドを使用します。

<#root>

leaf101#

show snmp summary

<

Admin State : enabled

, running (pid:26630)

Local SNMP engineID: [Hex] 8000000903003A9C451079
[Dec] 128:000:000:009:003:000:058:156:069:016:121

Community	Context	Status
snmp		ok

User	Authentication	Privacy	Status
snmpv3-user	hmac-sha2-256	none	ok

Admin State（管理状態）が有効で、Community（SNMPv1またはSNMPv2c）またはUser(SNMPv3)にエントリがある場合、SNMPが設定され、実行されています。Cisco Application Policy Infrastructure Controller(APIC)Web UIからのSNMP設定については、『ACIでのSNMPの設定』テクニカルノートを参照してください。

AAA 設定の確認

AAA設定を確認するには、APIC Web UIを使用して次の手順を実行します。

- Admin > AAAの順に選択します。
- [Authentication] をクリックします。
- Providersをクリックします。

AAAプロバイダーがIPv4アドレスの代わりにDNS名（ホスト名またはFQDN）またはIPv6アドレスを使用して設定されている場合、SNMPが有効でアクティブであれば、デバイスは脆弱な設定になります。

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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
- 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 200 シリーズ
- Cisco Secure Firewall 1200 シリーズ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- Cisco Secure Firewall 6100 シリーズ
- 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

- UCS 6600 シリーズ ファブリック インターコネクト
- UCS Xシリーズダイレクトファブリックインターコネクト9108 100G

セキュリティ侵害の痕跡

この脆弱性が悪用されると、SNMPdプロセスは、メモリ不足(OOM)状態によってカーネルパニックが発生し、デバイスがリロードされるまで、メモリを消費します。この問題を確認するには、スイッチのCLIから管理者権限で次のコマンドを使用します。

SNMPdプロセスの数を確認するには、ps -eaf | grep -i snmpdを使用します。

<#root>

Leaf101#

ps -eaf | grep snmpd

```
root     16944 18558  0 Aug08 ?        00:00:00 [snmpd] <defunct>
root     17523 18558  0 Aug08 ?        00:00:00 [snmpd] <defunct>
root     17859 18558  0 Aug08 ?        00:00:00 [snmpd] <defunct>
root     18036 18558  0 Aug08 ?        00:00:00 [snmpd] <defunct>
root     18558 12508  0 Aug08 ?        00:27:50 /isan/bin/snmpd -f -s -d udp:161 udp6:161 tcp:161
root     20075 18558  0 Aug08 ?        00:00:00
```

/isan/bin/snmpd -f -s -d udp:161 udp6:161 tcp:161

SNMPdプロセスの数が10を超え、時間の経過とともに増加している場合、デバイスはこの脆弱性の影響を受ける可能性があります。<defunct>と表示されるプロセスはメモリを消費しませんが、これもこの脆弱性を示している可能性があります。

未使用のメモリ使用量を取得するには、free -k | awk 'NR==2 {printf "Memory-used: %.2f%%\n", ($2-$7)/$2*100}'を使用します。

<#root>

Leaf101#

free -k | awk 'NR==2 {printf "Memory-used: %.2f%%\n", ($2-$7)/$2*100}'

Memory-used: 45.03%

メモリ使用量が85 %を超え、時間の経過とともに増加している場合は、デバイスがOOM状態に近づいており、リロードが発生する可能性があります。Cisco Technical Assistance Center(TAC)は、デバイスを高メモリ状態から回復するのに役立ちます。

回避策

この脆弱性の回避策は、IPv4 DNS名を使用して設定されているAAAプロバイダーに対して存在します。すべてのAAAプロバイダーをDNS名（ホスト名またはFQDN）からIPv4アドレス設定に更新します。AAA設定の詳細については、『Cisco Application Centric Infrastructure Fundamentals, Release 6.1(x)』を参照してください。

IPv6の設定に対する回避策はありません。

この回避策は、テスト環境に導入して問題なく実施できることが実証されていますが、お客様の環境や使用条件下での適用性と有効性を確認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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

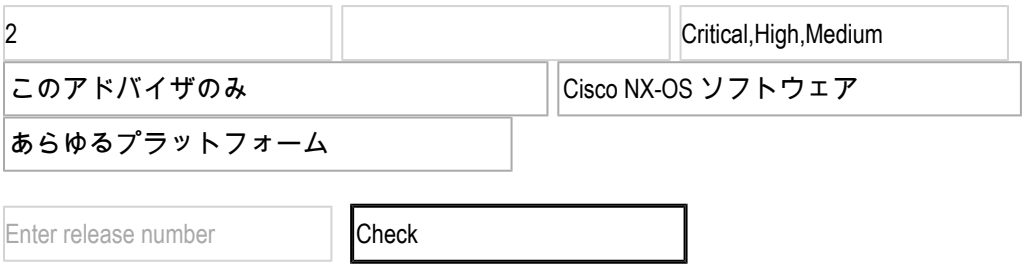
Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS 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 10.4(4)、ACI モードの Cisco NX-OS ソフトウェアの場合は 16.0(8e) です。

5. [チェック（Check）] をクリックします。



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
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-nxos-dsnmp-cNN39Uh

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	2026年2月25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。