Cisco NX-OS ソフトウェアの認証された Simple Network Management Protocol におけるサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20181017-nxos-snmp

初公開日 : 2018-10-17 16:00

バージョン 1.0 : Final

CVSSスコア : 7.7

回避策 : No workarounds available

Cisco バグ ID : CSCvj70029

CVE-2018-0456

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 NX-OS ソフトウェアにおける、Simple Network Management Protocol（SNMP）の入力パケット プロセッサの脆弱性により、認証されていないリモートの攻撃者が、該当デバイスの SNMP アプリケーションを予期せず再起動する可能性があります。

本脆弱性は、SNMP パケットにおける SNMP プロトコル データ単位（PDU）の不適切な入力検証に起因しています。 細工された SNMP パケットが該当デバイスに送信されると、本脆弱性がエクスプロイトされる危険性があります。 エクスプロイトが成功すると、攻撃者は、SNMP アプリケーションを複数回再起動させることにより、システム レベルの再起動とサービス妨害（DoS）状態を引き起こすことができます。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181017-nxos-snmp

該当製品

脆弱性のある製品

本脆弱性は、Cisco NX-OS ソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

- Nexus 3000 シリーズ スイッチ
- Nexus 3600 プラットフォーム 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 ラインカードおよびファブリック モジュール

スタンドアロン NX-OS モードの Nexus 3000 シリーズ スイッチと Nexus 9000 シリーズ スイッチ向けソフトウェア リリースでは、7.0(3)I7(3) にのみ脆弱性があります。

Nexus 3600 プラットフォーム スイッチ、および Nexus 9500 R シリーズのライン カードとファブリック モジュール向けソフトウェア リリースでは、7.0(3)F3(4) にのみ脆弱性があります。

影響を受けるリリースの詳細については、本セキュリティ 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 の状況を確認する

管理者は、デバイスの CLI で show running-config snmp コマンドを使用して、SNMP がデバイスで実行されているかどうかを確認できます。 コマンドによって出力が返された場合は、SNMP が設定されています。

```
nxos-switch# show running-config snmp
.
.
.
snmp-server user admin network-admin auth md5 ***** priv ***** localizedkey
snmp-server community community-string group network-admin
```

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 2100 シリーズ
- Firepower 4100 シリーズ次世代ファイアウォール
- 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 2000 シリーズ スイッチ
- Nexus 3500 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
- Nexus 9000 シリーズ ファブリック スイッチ (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)
- ユニファイド コンピューティング システム (UCS) 6100 シリーズ ファブリック インターコネクト
- 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

詳細

SNMP は、アプリケーションレイヤ プロトコルであり、ネットワーク デバイスのモニタリングや管理で、標準化されたフレームワークおよび共通言語として使用されます。 SNMP マネージャとエージェント間の通信に必要なメッセージ フォーマットを定義します。

SNMP エージェントは、デバイス パラメータおよびネットワーク データに関する情報のリポジトリである SNMP MIB からデータを収集します。 また、SNMP マネージャからの要求に応答して、データの取得または設定も行います。 SNMP エージェントには MIB 変数が含まれ、その値は、**get 操作**または **set 操作**を使用することによって、SNMP マネージャによって要求または変更できます。

本脆弱性は、デバイスでサポートされている SNMP のすべてのバージョン、つまり、バージョン 1、2c、3 に影響を与えます。 該当デバイスに IPv4 または IPv6 経由で特定の SNMP パケットが送信されると、本脆弱性がエクスプロイトされる危険性があります。 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。

SNMP バージョン 2c 以前で本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 SNMP 読み取り専用コミュニティ ストリングを把握している必要があります。 コミュニティ ストリングとは、デバイスの SNMP データへの読み取り専用アクセスおよび読み取り/書き込みアクセスの両方を制限するパスワードです。 コミュニティ ストリングには一般的なキーワードを使用せず、他のパスワードと同様に慎重に選択してください。 また、定期的にネットワーク セキュリティのポリシーに合わせて変更する必要もあります。 たとえば、ネットワーク管理者がロールを変更する場合や退職する際はコミュニティ ストリングを変更する必要があります。

SNMP バージョン 3 でこれらの脆弱性をエクスプロイトするには、該当システムのユーザ クレデンシャルを攻撃者が入手している必要があります。

回避策

この脆弱性に対処する回避策はありません。

このアドバイザリで述べている脆弱性の軽減策として、管理者は、SNMP コミュニティにアクセス コントロール リスト（ACL）を設定できます。 この ACL により、受信する SNMP 要求をフィルタリングし、信頼できる SNMP クライアントのみに SNMP ポーリングの実行を許可できます。 次の例では、192.168.1.2 と 192.168.1.3 の信頼できるホストから受信する SNMP 要求のみデバイスで許可されます。

```
switch# show access-list acl_for_snmp
IPV4 ACL acl_for_snmp 10 permit udp 192.168.1.2/32 192.168.1.3/32 eq snmp
```

前の ACL は、管理者が **snmp-server community** コンフィギュレーション コマンドに追加することで、実装することができます。

```
switch# show running-config snmp
snmp-server community mycompany use-acl acl_for_snmp
```

受信する SNMP 要求をフィルタリングする ACL の設定方法については、Cisco NX-OS 構成ガイドの Filtering SNMP Requests 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 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

次の表で、左の列は Cisco NX-OS ソフトウェアのリリースを示します。 右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けているかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。

スタンドアロン NX-OS モードの Nexus 3000 シリーズ スイッチおよび 9000 シリーズ スイッチ： CSCvj70029

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
7.0(3)I5 以前	脆弱性なし
7.0(3)I5	脆弱性なし
7.0(3)I6	脆弱性なし
7.0(3)I7	7.0(3)I7(4)
9.2(1)	脆弱性なし

Nexus 3600 プラットフォーム スイッチ、および 9500 R シリーズのライン カードとファブリック モジュール： CSCvj70029

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース
7.0(3)	ソフトウェア メンテナンス アップグレード（SMU）7.0(3)F3(4)
9.2(1)	脆弱性なし

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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181017-nxos-snmp

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-October-17

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したり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。