目次

概要

このドキュメントでは、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）の保護について説明します。 SNMP の脆弱性を利用してサービス拒絶（DoS）が繰り返し引き起こされる可能性がある場合は、特に SNMP を保護することが重要です。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- SNMP ビューか。Cisco IOS® ソフトウェア リリース 10.3 または それ 以降。
- Cisco IOS ソフトウェア リリース 12.0(3)T の SNMP バージョン 3?Introduced。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

SNMP を保護するための戦略

有効な SNMP コミュニティストリングを選択する

public を読み取り専用コミュニティ ストリングとして使用し、private を読み取りと書き込みコミュニティ ストリングとして使用するのは、有効な方法ではありません。

SNMP ビューのセットアップ

Setup SNMP view コマンドは、限定された Management Information Base (MIB; 管理情報ベース) へのアクセスしか持たないユーザをブロックすることができます。 デフォルトでは、**SNMP ビューのエントリ はありません**。 このコマンドはグローバル コンフィギュレーション モードで設定され、Cisco IOS ソフトウェア バージョン 10.3 で初めて導入されました。 特定の MIB ツリーに **SNMP ビュー** があると、1 つおきにツリーが拒否されるという不可解な動作に関して、このコマンドは **access-list** と似ています。 しかしシーケンスは重要でなく、リスト全体が検索され一致があったところで停止します。

ビューのエントリを作成または更新するには、**snmp-server view global configuration コマンド**を使用します。 指定された SNMP サーバ ビューのエントリを削除するには、このコマンドの **no 形式**を使用します。

構文：

```
snmp-server view view-name oid-tree {included | excluded} no snmp-server view view-name
```

構文の説明：

- **ビュー名**か。アップデートするか、または作成しているビュー レコードのためのラベル。 この名前は、レコードを参照するために使用します。
- **oid-tree** か。ビューから含まれているか、または除かれる抽象構文記法タイプ 1（抽象構文記法.1）サブツリーのオブジェクト識別子。 サブツリーを指定するには、1.3.6.2.4 のような数字で構成されるテキスト ストリング、または **system** のような語を使用します。 サブツリー ファミリを指定するには、1 つのサブ識別子をアスタリスク（*）ワイルドカードに置き換えます。 たとえば、1.3.*.4 とします。
- **included | 除かれる**か。ビューの型。 included または excluded のいずかを指定します。

ビューが必要な場合、ビューを定義するのではなく、事前定義された標準的な 2 つのビューを使用できます。 1 つは everything であり、ユーザはすべてのオブジェクトを表示できます。 もう 1 つは *restricted* であり、ユーザは次の 3 つのグループを表示できます。 **system**、**snmpStats**、および **snmpParties** です。 事前定義されたビューは、RFC 1447 で説明されています。

注最初の **snmp-server コマンド**の入力により、SNMP の両方のバージョンがイネーブルになります。

次の例では、MIB-II のシステム グループの **sysServices**（System 7）を除いたすべてのオブジェクトと、 MIB-II のインターフェイス グループのインターフェイス 1 のすべてのオブジェクトを含むビューを作成します。

```
snmp-server view agon system includedsnmp-server view agon system.7 excluded snmp-server view
agon ifEntry.*.1 included
```

次に MIB をコミュニティ ストリングに適用する方法と、**view** を指定した **snmpwalk** の出力の完全な例を示します。 この設定は、Address Resolution Protocol (ARP) テーブル (**atEntry**) で SNMP アクセスを拒否し、MIB-II およびシスコのプライベート MIB で SNMP アクセスを許可するビューを定義します。

```
snmp-server view myview mib-2 includedsnmp-server view myview atEntry excludedsnmp-server view myview cisco includedsnmp-server community public view myview RO 11snmp-server community private view myview RW 11snmp-server contact pvanderv@cisco.com
```

次に MIB-II System グループのコマンドと出力を示します。

```
NMSPrompt 82 % snmpwalk cough system system.sysDescr.0 : DISPLAY STRING- (ascii):Cisco Internetwork Operating System Software IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(1)T,RELEASE SOFTWARE (fc2) Copyright (c) 1986-1998 by cisco Systems, Inc. Compiled Wed 04-Nov-98 20:37 by dschwart system.sysObjectID.0 : OBJECT IDENTIFIER: .iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.cisco2520 system.sysUpTime.0 : Timeticks: (306588588) 35 days, 11:38:05.88 system.sysContact.0 : DISPLAY STRING- (ASCII):pvanderv@cisco.com system.sysName.0 : DISPLAY STRING- (ASCII):cough system.sysLocation.0 : DISPLAY STRING- (ASCII): system.sysServices.0 : INTEGER: 78 system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00 NMSPrompt 83 %
```

次にローカルの Cisco System グループのコマンドと出力を示します。

```
NMSPrompt 83 % snmpwalk cough lsystem cisco.local.lsystem.romId.0 : DISPLAY STRING- (ASCII): System Bootstrap, Version 11.0(10c), SOFTWARE Copyright (c) 1986-1996 by cisco Systems cisco.local.lsystem.whyReload.0 : DISPLAY STRING- (ASCII):power-on cisco.local.lsystem.hostName.0 : DISPLAY STRING- (ASCII):cough
```

次に MIB-II ARP テーブルのコマンドと出力を示します。

```
NMSPrompt 84 % snmpwalk cough atTable no MIB objects contained under subtree. NMSPrompt 85 %
```

アクセスリストで SNMP コミュニティをセットアップする

現在のベスト プラクティスでは、Access Control Lists (ACL; アクセス コントロール リスト) をコミュニティ ストリングに適用し、要求コミュニティ ストリングと通知コミュニティ ストリングを同一にしないことが推奨されています。 アクセス リストを他の保護措置と組み合わせて使用すれば、保護機能が高められます。

次に ACL をコミュニティ ストリングに設定する例を示します。

```
access-list 1 permit 1.1.1.1 snmp-server community string1 ro 1
```

要求とトラップ メッセージに異なったコミュニティ ストリングを使用すれば、攻撃者がリモート デバイスに侵入したり権限なしにネットワークからトラップ メッセージをスニッフィングしてコミュニティ ストリングを読み取ったとしても、それ以上の攻撃や侵入を受ける可能性が少なくなります。

一部の Cisco IOS ソフトウェアでは 、一度コミュニティ ストリングでトラップをイネーブルすれば、SNMP アクセスでそのストリングがイネーブルされます。 このコミュニティは明示的にディセーブルする必要があります。

次に、例を示します。

```
access-list 10 deny any snmp-server host 1.1.1.1 mystring1 snmp-server community mystring1 RO 10
```

SNMP バージョン 3 のセットアップ

SNMPバージョン 3 は Cisco IOS ソフトウェア バージョン 12.0 で初めて導入されましたが、ネットワーク管理ではまだ一般的に使用されていません。 SNMP バージョン 3 を設定するには、次の手順を実行します。

1. SNMP エンティティのエンジン ID を割り当てます（オプション）。
2. **groupone** グループに属する **userone** ユーザを定義し、このユーザに **noAuthentication**（パスワードなし）および **noPrivacy**（暗号化なし）を適用します。
3. **grouptwo** グループに属する **usertwo** ユーザを定義し、このユーザに **noAuthentication**（パスワードなし）および **noPrivacy**（暗号化なし）を適用します。
4. **groupthree** グループに属する **userthree** ユーザを定義し、このユーザに **Authentication**（パスワードは user3passwd）および **noPrivacy**（暗号化なし）を適用します。
5. **groupfour** グループに属する **userfour** ユーザを定義し、このユーザに **Authentication**（パスワードは user4passwd）および **Privacy**（des56 暗号化方式）を適用します。
6. User-based Security Model (USM; ユーザベース セキュリティ モデル) V3 を使用して、**v1default** ビュー（デフォルト）での読み取りアクセスを持つ **groupone** グループを定義します。
7. USM V3 を使用して、**myview** ビューでの読み取りアクセスを持つ **grouptwo** グループを定義します。
8. USM V3 を使用して、**v1default** ビュー（デフォルト）での読み取りアクセスを持ち、**authentication** を使用するグループ **groupthree** グループを定義します。
9. USM V3 を使用して、**v1default** ビュー（デフォルト）での読み取りアクセスを持ち、**Authentication** および **Privacy** を使用する **groupfour** グループを定義します。
10. MIB-II での読み取りアクセスを提供し、プライベートな Cisco MIB での読み取りアクセスを拒否する **myview** ビューを定義します。読み取り専用コミュニティ ストリング **public** が定義されているため、**show running** の出力には **public** グループの行も含まれます。**show running** の出力には、**userthree** は表示されません。例：**snmp-server engineID local 111100000000000000000000snmp-server user userone groupone v3 snmp-server user usertwo grouptwo v3 snmp-server user userthree groupthree v3 auth md5 user3passwd snmp-server user userfour groupfour v3 auth md5 user4passwd priv des56 user4priv snmp-server group groupone v3 noauth snmp-server group grouptwo v3 noauth read myview snmp-server group groupthree v3 auth snmp-server group groupfour v3 priv snmp-server view myview mib-2 included snmp-server view myview cisco excluded snmp-server community public RO**

これは、**userone** ユーザを使用した MIB-II System グループのコマンドと出力です。

```
NMSPrompt 94 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy system Module SNMPV2-TC not
found system.sysDescr.0 = Cisco Internetwork Operating System Software IOS (TM) 4500 Software
(C4500-IS-M), Version 12.0(3)T,RELEASE SOFTWARE (fc1) Copyright (c) 1986-1999 by cisco Systems,
Inc. Compiled Tue 23-Feb-99 03:59 by ccai system.sysObjectID.0 = OID: enterprises.9.1.14
system.sysUpTime.0 = Timeticks: (28208096) 3 days, 6:21:20.96 system.sysContact.0 =
system.sysName.0 = clumsy.cisco.com system.sysLocation.0 = system.sysServices.0 = 78
system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00NMSPrompt 95 %
```

これは、**usertwo** ユーザを使用した MIB-II System グループのコマンドと出力です。

```
NMSPrompt 95 % snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy system  Module SNMPV2-TC not
found system.sysDescr.0 = Cisco Internetwork Operating System Software IOS (TM) 4500 Software
(C4500-IS-M), Version 12.0(3)T,RELEASE SOFTWARE (fc1) Copyright (c) 1986-1999 by cisco Systems,
Inc. Compiled Tue 23-Feb-99 03:59 by ccai system.sysObjectID.0 = OID: enterprises.9.1.14
system.sysUpTime.0 = Timeticks: (28214761) 3 days, 6:22:27.61 system.sysContact.0 =
system.sysName.0 = clumsy.cisco.com system.sysLocation.0 = system.sysServices.0 = 78
system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00
```

これは、**userone** ユーザを使用した Cisco Local System グループのコマンドと出力です。

```
NMSPrompt 98 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy .1.3.6.1.4.1.9.2.1  Module
SNMPV2-TC not found enterprises.9.2.1.1.0 = "..System Bootstrap, Version 5.2(7b) [mkamson 7b],
RELEASE SOFTWARE (fc1)..Copyright (c) 1995 by cisco Systems,Inc..." enterprises.9.2.1.2.0 =
"reload"enterprises.9.2.1.3.0 = "clumsy"enterprises.9.2.1.4.0 = "cisco.com"
```

これは、ユーザ **usertwo** を使用して Cisco Local System グループを取得できないことを示すコマンドと出力です。

```
NMSPrompt 99 % snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy .1.3.6.1.4.1.9.2.1  Module
SNMPV2-TC not found enterprises.9.2.1 = No more variables left in this MIB View NMSPrompt 100 %
```

次にカスタマイズした tcpdump（SNMP バージョン 3 のサポートと printf 追補のパッチ）のコマンドと出力結果を示します。

```
NMSPrompt 102 % snmpget -v3 -n "" -u userone -l noAuthNoPriv clumsy system.sysName.0 Module
SNMPV2-TC not found system.sysName.0 = clumsy.cisco.com
```

インターフェイスでの ACL 設定

ACL 機能は、IP スプーフィングなどの攻撃を防ぐためのセキュリティ対策になります。 ACL はルータの着信インターフェイスまたは発信インターフェイスに適用できます。

受信 ACL（rACL）を使用するオプションのないプラットフォームでは、インターフェイス ACL を使用して、信頼できる IP アドレスからルータへの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トラフィックを許可することができます。

次の拡張アクセス リストをネットワークに適用できます。 次の例での前提事項は、ルータのインターフェイスに IP アドレス 192.168.10.1 および 172.16.1.1 が設定されていること、すべての SNMP アクセスが IP アドレス 10.1.1.1 の管理ステーションに限定されていること、およびその管理ステーションが IP アドレス192.168.10.1とだけ通信する必要があることです。

```
access-list 101 permit udp host 10.1.1.1 host 192.168.10.1
```

ここで、次の設定コマンドを使用し、 access-list をすべてのインターフェイスに適用する必要があります。

```
interface ethernet 0/0ip access-group 101 in
```

UDP ポートで直接ルータと通信を行うデバイスはすべて、上のアクセスリストに明確に記載される必要があります。 Cisco IOS ソフトウェアは、49152 から 65535 までの範囲のポートを Domain Name System（DNS; ドメイン ネーム システム）クエリーなどのアウトバウンド セッションのソース ポートに使用します。

IP アドレスが多数設定されているデバイス、またはルータと通信する必要がある多数のホストでは、この方法はスケーラブルなソリューションでない場合があります。

受信 ACL（rACL）

分散プラットフォームでは、Cisco 12000 シリーズ ギガビット スイッチ ルータ（GSR）の Cisco IOS ソフトウェア リリース 12.0(21)S2、および Cisco 7500 シリーズのリリース 12.0(24)S からのオプションとして、rACL が適しているかもしれません。 受信アクセス リストは、ルート プロセッサが有害なトラフィックの影響を受ける前に、そのトラフィックからデバイスを保護します。 受信パス ACL もネットワーク セキュリティのベスト プラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、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べきです。 CPU 負荷がライン カード プロセッサに分散されるため、メイン ルート プロセッサの負荷を軽減させるのに役立ちます。 『GSR： 受信アクセス コントロール リスト』というタイトルのホワイト ペーパーは、正当なトラフィックを識別してデバイスに許可を与え、望ましくないパケットをすべて拒否するのに役立ちます。

インフラストラクチャ ACL

ネットワークを移動するトラフィックをブロックするのは往々にして困難ですが、インフラストラクチャ デバイスに送られてはならないトラフィックを識別し、ネットワークの境界でそのトラフィックをブロックすることは可能です。 インフラストラクチャ ACL（iACL）はネットワーク

セキュリティのベスト プラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、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べきです。 『コアの保護： インフラストラクチャ保護 ACL』というタイトルのホワイト ペーパーには、iACL についてのガイドラインと推奨される配備方法が説明されています。

Cisco Catalyst LAN スイッチのセキュリティ機能

IP 許可リスト機能は、権限のない送信元 IP アドレスからスイッチへの着信 Telnet アクセスおよび SNMP アクセスを制限します。 違反または不正アクセスが発生したときに管理システムに通知するため、syslog メッセージと SNMP トラップがサポートされています。

ルータと Cisco Catalyst スイッチの管理には、Cisco IOS ソフトウェアのセキュリティ機能を組み合わせて使用できます。 スイッチとルータにアクセスできる管理ステーションの数を制限するセキュリティ ポリシーを確立する必要があります。

IP ネットワークのセキュリティを強化する方法の詳細については、『IP ネットワークでのセキュリティ強化』を参照してください。

SNMP エラーをチェックする方法

log キーワードを使用して、 SNMP コミュニティ ACL を設定します。 次のように、失敗した試行について **syslog** を監視します。

```
access-list 10 deny any log snmp-server community public RO 10
```

誰かがコミュニティ public でルータにアクセスしようとした場合、**syslog** には次のように表示されます。

```
access-list 10 deny any log snmp-server community public RO 10
```

この出力は、アクセス リスト 10 がホスト 172.16.1.1 からの SNMP パケットを 5 つ拒否したことを意味します。

次のように、**show snmp コマンド**を実行して SNMP にエラーがないかを定期的に確認します。

```
router#show snmp Chassis: 21350479 17005 SNMP packets input 37 Bad SNMP version errors**15420
Unknown community name**0 Illegal operation for community name supplied 1548 Encoding errors**0
Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0
Set-request PDUs 0 SNMP packets output 0 Too big errors (Maximum packet size 1500) 0 No such
name errors 0 Bad values errors 0 General errors 0 Response PDUs 0 Trap PDUs
```

** マークのあるカウンタを監視し、エラー率が予想以上に増加していたら、脆弱性を利用する試みが行われている可能性があります。 セキュリティ問題を報告するには、『シスコのセキュリティ問題対応製品』を参照してください。

関連情報

- Cisco セキュリティ アドバイザリ SNMP の脆弱性
- IOS 12.0 による SNMP v3 の設定
- 簡易ネットワーク管理プロトコル (SNMP)
- SNMP の設定
- テクニカルサポート - Cisco Systems