提高简单网络管理协议的安全性

目录

简介

本文提供信息保护您的简单网络管理协议(SNMP)。特别是当SNMP的漏洞可以重复被利用导致拒绝服务时，保护您的SNMP是重要。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- SNMP视图— Cisco IOS软件版本10.3或以上。
- SNMP版本3 —介绍在Cisco IOS软件版本12.0(3)T。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

保护 SNMP 的策略

选择好的 SNMP 社区字符串

它不是良好的做法使用**公共**一样只读和**私有**象读写团体串。

设置 SNMP 视图

Setup SNMP view命令能阻塞有仅访问的用户对有限的管理信息库(MIB)。默认情况下，没有**View条目的SNMP存在**。此命令在Cisco IOS软件版本10.3配置在全局配置模式和首先介绍。它工作类似于**access-list**由于，如果有在某些MIB树的任何**SNMP视图**，其他树莫名奇妙地拒绝。然而，顺序不是重要，并且通过匹配的整个列表，在终止前。

要创建或更新View条目，请使用**snmp-server view global configuration命令**。要删除View条目指定的SNMP的服务器，请使用此命令**no表示**。

语法：

```
snmp-server view view-name oid-tree {included | excluded}

no snmp-server view view-name
```

语法说明：

- **视图NAME** —您更新或创建的视图记录的标签。名称用于参考记录。
- **oid-tree** —从视图将包括或排除的抽象语法标记(ASN.1)子树的对象标识符。要识别子树，请指定文本字符串包括编号，例如1.3.6.2.4的或者一个词，例如**系统**。用星号(*)通配符替换单个子标识指定子树家族;例如1.3.*.4。
- **包括|不包括**—视图的类型。您必须指定包括或排除。

两张标准预定义的视图可以使用，当视图要求时，而不是定义视图。一个是一切，表明用户能看到所有对象。其他*限制*，表明用户能看到三组：**系统**、**snmpStats**和**snmpParties**。预定义的视图在RFC 1447描述。

注意： 第一**snmp-server命令**您参与enable (event) SNMP两个版本。

此示例创建在MIB II系统组包括所有对象除了**sysServices的**视图(系统7)和接口的1所有对象在MIB-II接口组：

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

snmp-server view agon ifEntry.*.1 included
```

这是如何的一完整示例能应用与社区字符串和**snmpwalk的**输出的MIB与到位**视图的**。此配置定义了拒绝地址解析服务(ARP)表的视图(**atEntry**) SNMP访问并且允许它MIB-II和思科私有MIB ：

```
snmp-server view myview mib-2 included

snmp-server view myview atEntry excluded

snmp-server view myview cisco included

snmp-server community public view myview RO 11

snmp-server community private view myview RW 11

snmp-server contact pvanderv@cisco.com
```

这是命令和输出MIB II系统组的：

```
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 %
```

这是命令和输出活动进程系统组的：

```
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
```

这是命令和输出MIB-II ARP表的：

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

使用 access-list 设置 SNMP团体

最好的当前运作推荐应用访问控制列表(ACL)到社区字符串和保证请求社区字符串与通知社区字符串不是相同的。访问列表提供进一步防护，当使用与其他保护措施的组合。

此示例设置ACL对社区字符串：

```
access-list 1 permit 1.1.1.1

snmp-server community string1 ro 1
```

使用请求和陷阱消息的不同的社区字符串降低深层攻击或妥协可能性，如果社区字符串发现由攻击者，还是减弱远程设备或通过探测从网络的一个陷阱消息，不用授权。

一旦启用有社区字符串的陷阱，字符串在若干Cisco IOS软件方面可能为SNMP访问启用。您必须明确地禁用此社区。

例如：

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

设置 SNMP 版本3

SNMP版本3在Cisco IOS软件版本12.0首先介绍，但是不是常用的在网络管理方面。要配置SNMP版本3，请完成这些步骤：

1. 为SNMP实体分配引擎ID (可选)。
2. 定义用户， **userone**，属于组**groupone**并且应用**noAuthentication** (没有密码)和**noPrivacy** (不加密)给此用户。
3. 定义用户， **usertwo**，属于组**grouptwo**并且应用**noAuthentication** (没有密码)和**noPrivacy** (不加密)给此用户。
4. 定义用户， **userthree**，属于组**groupthree**并且应用**验证**(密码是user3passwd)和**noPrivacy** (不加密)给此用户。
5. 定义用户， **userfour**，属于组**groupfour**并且应用**验证**(密码是user4passwd)和**保密性**(des56加密)给此用户。
6. 定义组， **groupone**，使用用户安全模式(USM) V3和在**v1default**视图(默认)的访问读访问。
7. 使用USM V3和在视图**myview**的访问读访问定义组， **grouptwo**。
8. 使用USM V3，定义组， **groupthree**，访问在**v1default**视图(默认)的读访问和使用**验证**。

9. 使用USM V3，定义组， **groupfour**，访问在**v1default**视图(默认)的读访问和使用**验证**和**保密性**。
10. 定义视图， **myview**，在MIB-II提供读访问并且拒绝在私有Cisco MIB的读访问。**show running**输出给组**公共的**另外的线路，由于这样的事实有定义的社区字符串只读**公共**。**show running**输出不显示**userthree**。**示例：**

```
snmp-server engineID local 1111000000000000000000
snmp-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
```

使用用户**userone**，这是命令和输出MIB II系统组的：

```
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) 0:00:00.00
NMSPrompt 95 %
```

使用用户**usertwo**，这是命令和输出MIB II系统组的：

```
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
```

这是命令和输出使用用户**userone的**思科本地系统组的：

```
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"
```

这是命令，并且显示您的输出不能获得使用用户**usertwo的**思科本地系统组：

```
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 %
```

此命令和产生的输出是为一定制的**tcpdump** (SNMP版本3 printf支持和附录的补丁程序) ：

```
NMSPrompt 102 % snmpget -v3 -n "" -u userone -l noAuthNoPriv clumsy system.sysName.0

Module SNMPV2-TC not found
system.sysName.0 = clumsy.cisco.com
```

在接口的设置ACL

在防止攻击的ACL功能提供安全措施例如IP伪装。ACL在路由器的流入或流出的接口可以应用。

在没有选项使用receive ACL (rACL)的平台上，允许用户数据报协议(UDP)流量到从委托IP地址的路由器与接口ACL是可能的。

以下扩展访问列表可以适应您的网络。此示例假设，路由器有IP地址在其接口和172.16.1.1配置的192.168.10.1，所有SNMP访问将限制到一个管理站用10.1.1.1的IP地址，并且管理站需要与IP地址192.168.10.1只联络：

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

使用这些配置命令， **access-list**必须然后应用到所有接口：

```
interface ethernet 0/0
```

```
ip access-group 101 in
```

直接地与在UDP端口的路由器联络的所有设备在上述访问列表将需要特别地列出。Cisco IOS软件在范围49152到65535使用端口作为呼出会话的源端口例如域名系统(DNS)查询。

对于有配置的许多IP地址的设备，或者需要用路由器通信的许多主机，这可能不是可扩展的解决方案。

rACL

对于分布式平台， rACL可能是开始在Cisco 12000系列gigabit交换机路由器(GSR)和版本的12.0(24)S Cisco IOS软件版本12.0(21)S2的选项Cisco 7500系列的。在流量能影响路由处理器前，接收访问列表保护从有害流量的设备。接收路径ACL也认为网络安全最佳实践，并且应该考虑作为对好网络安全的一长期新增内容，以及此特定漏洞的一应急方案。CPU负载被分配到线路卡处理器，并且帮助缓和在主路由处理器的负载。标题名为GSR的白皮书：接收访问控制列表将帮助识别和允许合法数据流到您的设备和丢弃所有不需要的数据包。

基础架构 ACL

虽然阻塞传输您的网络的流量经常是难的，识别不应该允许在您的网络边界瞄准您的基础设备和块该流量的流量是可能的。基础设施ACL (iACLs)认为网络安全最佳实践，并且应该考虑作为对好网络安全的一长期新增内容以及此特定漏洞的一应急方案。题为的白皮书保护您的核心：基础设施保护访问控制列出存在指南和推荐的部署技术的iACLs。

思科Catalyst LAN交换机安全特性

ip permit列表功能限制从未授权的源IP地址到交换机的Inbound Telnet和SNMP访问。当发生违规或未经授权的访问时，支持系统日志消息和SNMP陷阱通知到管理系统。

Cisco IOS软件安全功能的组合可以用于管理路由器和思科Catalyst交换机。需要建立安全策略，以限制能够访问交换机和路由器的管理站的数量。

关于如何强化在IP网络的安全的更多信息，参考增强IP网络安全。

如何检查 SNMP 错误

配置与**日志关键字的**SNMP团体ACL。监控失败的尝试的**Syslog**，和显示下面。

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

当某人设法访问有属性公有的时路由器，您看到**Syslog**类似于以下：

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

此输出意味着access-list 10拒绝从主机172.16.1.1的五SNMP数据包。

周期地请检查SNMP错误由执行**show snmp命令**，如显示此处：

```
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
```

观看为在可能指示这些漏洞试图非法的错误率的意外的增量标记的**计数器。要报告所有安全问题，参考Cisco产品安全事件响应。

相关信息

- Cisco安全建议SNMP漏洞
- 与IOS 12.0的设置SNMP v3
- 简单网络管理协议 (SNMP)
- 配置SNMP
- 技术支持 - Cisco Systems