Secure Your Simple Network Management Protocol

Contents

Introduction

This document describes how to secure your Simple Network Management Protocol (SNMP).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- SNMP View — Cisco IOS® Software Release 10.3 or later.
- SNMP version 3 — Introduced in Cisco IOS Software Release 12.0(3)T.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Background Information

It is important to secure your SNMP especially when the vulnerabilities of SNMP can be repeatedly exploited to produce a denial of service (DoS).

Strategies to Secure SNMP

Choose a Good SNMP Community String

It is not a good practice to use **public** as read-only and **private** as read-write community strings.

Setup SNMP View

The Setup SNMP view command can block the user with only access to limited Management Information Base (MIB). By default, there is no SNMP view entry exists . This command is configured at the global configuration mode and first introduced in Cisco IOS Software version 10.3. It works similar to access-list in that if you have any SNMP View on certain MIB trees, every other tree is denied inexplicably. However, the sequence is not important and it goes through the entire list for a match before it stops.

To create or update a view entry, use the snmp-server view global configuration command. To remove the specified SNMP server view entry, use the no form of this command.

Syntax:

<#root>

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

```
no snmp-server view view-name
```

Syntax Description:

- view-name— Label for the view record that you update or create. The name is used to reference the record.
- oid-tree — Object identifier of the Abstract Syntax Notation One (ASN.1) subtree to be included or excluded from the view. To identify the subtree, specify a text string that consists of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- included | excluded— Type of view. You must specify either included or excluded.

Two standard predefined views can be used when a view is required instead of a view that must be defined. One is everything, which indicates that the user can see all objects. The other is *restricted* , which indicates that the user can see three groups: system, snmpStats, and snmpParties. The predefined views are described in RFC 1447.

Note: The first snmp-server command that you enter enables both versions of SNMP.

This example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
<#root>

snmp-server view agon system included


snmp-server view agon system.7 excluded


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

This is a complete example for how to apply the MIB with community string and the output of the snmpwalk with view in place. This configuration defines a view that denies the SNMP access for the Address Resolution Protocol (ARP) table (atEntry) and allows it for MIB-II and Cisco private MIB:

```
<#root>

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
```

This is the command and output for the MIB-II System group:

```
<#root>

NMSPrompt 82 %

snmpwalk cough system


system.sysDescr.0 : DISPLAY STRING- (ascii):Cisco Internetwork Operating System Software
Cisco 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 %
```

This is the command and output for the local Cisco System group:

```
<#root>

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
```

This is the command and output for the MIB-II ARP table:

```
<#root>

NMSPrompt 84 %

snmpwalk cough atTable


no MIB objects contained under subtree.
```

```
NMSPrompt 85 %
```

Setup SNMP Community with Access-list

The best current practices recommend that you apply Access Control Lists (ACLs) to community strings and ensure that the requests community strings are not identical to notifications community strings. Access lists provide further protection when used in combination with other protective measures.

This example sets up ACL to community string:

```
<#root>

access-list 1 permit 10.1.1.1



snmp-server community string1 ro 1
```

When you use different community strings for requests and trap messages, it reduces the likelihood of further attacks or compromises if the community string is discovered by an attacker. Otherwise, an attacker could compromise a remote device or sniff a trap message from the network without authorization.

Once you enable trap with a community string, the string can be enabled for SNMP access in some Cisco IOS software. You must explicitly disable this community. For example:

```
<#root>

access-list 10 deny any

snmp-server host 10.1.1.1 mystring1



snmp-server community mystring1 RO 10
```

Setup SNMP Version 3

Do these steps to configure SNMP version 3:

1. Assign an Engine ID for the SNMP Entity (Optional).
2. Define a user, **userone** that belongs to the group **groupone** and apply **noAuthentication** (no password) and **noPrivacy** (no encryption) to this user.
3. Define a user, **usertwo ;**that belongs the group **grouptwo** and apply **noAuthentication** (no password) and **noPrivacy** (no encryption) to this user.

4. Define a user, **userthree** that belongs the group **groupthree** and apply **Authentication** (password is user3passwd) and **noPrivacy** (no encryption) to this user.

5. Define a user, **userfour** , that belongs to the group **groupfour** and apply **Authentication** (password is user4passwd) and **Privacy** (des56 encryption) to this user.

6. Define a group, **groupone** , by means of User Security Model (USM) V3 and enable read access on the **v1default** view (the default).

7. Define a group, **grouptwo** , by means of USM V3 and enable read access on the view **myview** .

8. Define a group, **groupthree** , by means of USM V3, and enable read access on the **v1default** view (the default), by means of **authentication** .

9. Define a group, **groupfour** , by means of USM V3, and enable read access on the **v1default** view (the default), by means of **Authentication** and **Privacy** .

10. Define a view, **myview** , that provides read access on the MIB-II and denies read access on the private Cisco MIB.

    The show running output gives additional lines for the group **public**, due to the fact that there is a community string Read-Only **public** that has been defined.

    The show running output does not show the **userthree**.

Example:

<#root>

```
snmp-server engineID local 1111000000000000000000000
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
```

This is the command and output for the MIB-II System group with user **userone**:

<#root>

```
NMSPrompt 94 %

snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy system


Module SNMPV2-TC not found
system.sysDescr.0 = Cisco Internetwork Operating System Software
Cisco 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 %
```

This is the command and output for the MIB-II System group with user **usertwo**:

```
<#root>

NMSPrompt 95 %

snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy system
```

```
Module SNMPV2-TC not found
system.sysDescr.0 = Cisco Internetwork Operating System Software
Cisco 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
```

This is the command and output for the Cisco Local System group with user **userone**:

```
<#root>

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"
```

This is the command and output that shows you cannot get the Cisco Local System group with user

usertwo:

```
<#root>

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 %
```

This command and the output result is for a customized tcpdump (patch for SNMP version 3 support and addendum of printf):

```
<#root>

NMSPrompt 102 %

snmpget -v3 -n "" -u userone -l noAuthNoPriv clumsy system.sysName.0


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

Setup ACL on Interfaces

The ACL feature provides security measures that prevent attacks such as IP spoofing. The ACL can be applied on incoming or outgoing interfaces on routers.

On platforms that do not have the option to use receive ACLs (rACLs), it is possible to permit User Datagram Protocol (UDP) traffic to the router from trusted IP addresses with interface ACLs.

The next extended access list can be adapted to your network. This example assumes that the router has IP addresses 192.168.10.1 and 172.16.1.1 configured on its interfaces, that all SNMP access is to be restricted to a management station with the IP address of 10.1.1.1, and that the management station need only communicate with IP address 192.168.10.1:

```
<#root>

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

The access-list must then be applied to all interfaces with these configuration commands:

<#root>

```
interface ethernet 0/0

ip access-group 101 in
```

All devices that communicate directly with the router on UDP ports need to be specifically listed in the previous access list. Cisco IOS software uses ports in the range 49152 to 65535 as the source port for outbound sessions such as Domain Name System (DNS) queries.

For devices that have many IP addresses configured, or many hosts that need to communicate with the router, this is not always a scalable solution.

rACLs

For distributed platforms, rACLs can be an option that starts in Cisco IOS Software Release 12.0(21)S2 for the Cisco 12000 Series Gigabit Switch Router (GSR) and Release 12.0(24)S for the Cisco 7500 Series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path ACLs also are considered a network security best practice, and must be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled GSR: Receive Access Control Lists helps to identify legitimate traffic. Use that white paper to understand how to send legitimate traffic to your device and also deny all unwanted packets..

Infrastructure ACLs

Although it is often difficult to block traffic that transits your network, it is possible to identify traffic that must never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs (iACLs) are considered a network security best practice and must be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper, Protecting Your Core: Infrastructure Protection Access Control Lists ,presents guidelines and recommended deployment techniques for iACLs..

Cisco Catalyst LAN Switch Security Feature

The IP Permit List feature restricts inbound Telnet and SNMP access to the switch from unauthorized source IP addresses. Syslog messages and SNMP traps are supported to notify a management system when a violation or unauthorized access occurs.

A combination of the Cisco IOS software security features can be used to manage routers and Cisco Catalyst switches. A security policy needs to be established that limits the number of management stations that can access the switches and routers.

For more information on how to increase security on IP networks, refer to Increasing Security on IP Networks .

How to Check SNMP Errors

Configure the SNMP community ACLs with the log keyword. Monitor syslog for failed attempts, as show below.

<#root>

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

When someone tries to access the router with the community public, you see a syslog similar to this:

```
%SEC-6-IPACCESSLOGS: list 10 denied 172.16.1.15packet
```

This output means that access-list 10 has denied five SNMP packets from the host 172.16.1.1.

Periodically check SNMP for errors with the show snmp command, as shown here:

<#root>

```
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
```

Watch the counters marked ** for unexpected increases in error rates that can indicate attempted exploitation of these vulnerabilities. To report any security issue, refer to Cisco Product Security Incident Response.

Related Information

- **Cisco Security Advisories SNMP Vulnerabilities**
- **Cisco Technical Support & Downloads**