

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Estrategias para asegurar el SNMP](#)

[Elija una cadena de comunidad SNMP correcta](#)

[Setup SNMP view](#)

[Configuración de comunidad de SNMP con lista de acceso](#)

[Configurar SNMP Versión 3](#)

[Ponga el ACL en las interfaces](#)

[rACLs](#)

[ACL de Infraestructura](#)

[Función de seguridad de Cisco Catalyst LAN Switch](#)

[Cómo verificar errores SNMP](#)

[Información Relacionada](#)

Introducción

Este documento proporciona información sobre la protección de SNMP (Simple Network Management Protocol). La protección de SNMP es importante, especialmente cuando las vulnerabilidades de SNMP se pueden explotar en varias ocasiones para producir una Negación de servicio (DoS).

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ¿Opinión SNMP? Software Release 10.3 o Posterior de Cisco IOS®.
- Versión de SNMP 3? Introducida en el Cisco IOS Software Release 12.0(3)T.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

Estrategias para asegurar el SNMP

Elija una cadena de comunidad SNMP correcta

No es una práctica adecuada utilizar el **público** como solo lectura y **privado** como cadenas de comunidad de lectura/escritura.

Setup SNMP view

El comando **Setup SNMP view** puede bloquear al usuario con solamente el acceso al Management Information Base limitado (MIB). Por abandono, hay ningún **entrada ver SNMP existe**. Este comando se configura en el modo de configuración global y primero se introduce en la versión del Cisco IOS Software 10.3. Trabaja similar a la **lista de acceso** en eso si usted tiene cualquier **opinión SNMP** sobre ciertos árboles de MIB, cada otro árbol se niega inexplicablemente. Sin embargo, la secuencia no es importante y pasa a través de la lista entera para una coincidencia antes de que pare.

Para crear o poner al día una entrada de la visión, utilice el **comando snmp-server view global configuration**. Para quitar la entrada especificada de la opinión del servidor SNMP, no utilice la **ninguna** forma de este comando.

Sintaxis:

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

Descripción de la sintaxis:

- **¿vista-nombre?** Escritura de la etiqueta para el expediente de la visión que usted está poniendo al día o está creando. El nombre se utiliza para hacer referencia al registro.
- **¿OID-árbol?** Identificador de objeto de la sub-estructura del Abstract Syntax Notation One (ASN.1) que se incluirá o excluida de la visión. Para identificar el subárbol, especifique una cadena de texto que contenga números, como 1.3.6.2.4, o una palabra, como sistema. Substituya un solo sub-identificador por el comodín del asterisco (*) para especificar a una familia de subárbol; por ejemplo 1.3.*.4.
- **incluido | ¿excluido?** Tipo de visión. Usted debe especificar incluido o excluido.

Dos vistas predefinidas estándares se pueden utilizar cuando se requiere una visión, en vez de definir una opinión. Uno es *todo*, que indica que el usuario puede ver todos los objetos. El otro es *restringido*, que indica que el usuario puede ver a tres grupos: **sistema**, **snmpStats**, y **snmpParties**. Las vistas predefinidas se describen en el RFC 1447.

Nota: El primer **comando snmp-server** que usted ingresa habilita ambas versiones del SNMP.

Este ejemplo crea una visión que incluya todos los objetos en grupo de sistema MIB-II a excepción de los **sysServices** (sistema 7) y todos los objetos para la interfaz 1 en el grupo de las interfaces MIB-II:

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

Esto es un ejemplo completo para que cómo aplique el MIB con la cadena de comunidad y la salida del **snmpwalk** con la **visión** en el lugar. Esta configuración define una opinión que niegue el acceso SNMP para la tabla del Address Resolution Protocol (ARP) (**atEntry**) y lo permita para el soldado MIB MIB-II y de Cisco:

```
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
```

Ésta es el comando y la salida para grupo de sistema MIB-II:

```
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 dschwartz 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 %
```

Ésta es el comando y la salida para el grupo del sistema de Cisco local:

```
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
```

Ésta es el comando y la salida para la tabla ARP MIB-II:

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

[Configuración de comunidad de SNMP con lista de acceso](#)

Las mejores prácticas actuales recomiendan el aplicar del Listas de control de acceso (ACL) a las cadenas de comunidad y el asegurarse de que las cadenas de comunidad de las peticiones no son idénticas a las cadenas de comunidad de las notificaciones. Las Listas de acceso proporcionan la protección adicional cuando están utilizadas conjuntamente con otras medidas de protección.

Este ejemplo configura el ACL a la cadena de comunidad:

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

Usando diversas cadenas de comunidad para las peticiones y los mensajes trampa reduce la probabilidad de los otros ataques o de los compromisos si la cadena de comunidad es descubierta por un atacante, sea por el compromiso de un dispositivo remoto u oliendo un mensaje trampa de la red sin la autorización.

Una vez que usted habilita el desvío con una cadena de comunidad, la cadena se puede habilitar para el acceso SNMP en un cierto Cisco IOS Software. Usted debe inhabilitar explícitamente a esta comunidad.

Por ejemplo:

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

[Configurar SNMP Versión 3](#)


```
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 (fcl)..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"
```

Éste es el comando y la salida que le muestra no puede conseguir al grupo del sistema local de Cisco que usa el **usertwo** del usuario:

```
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 %
```

Este comando y salida resultante está para un **tcpdump** personalizado (corrección para el soporte del SNMP versión 3 y el addendum del printf):

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

[Configuración ACL en las interfaces](#)

La característica ACL proporciona medidas de seguridad ya que previene ataques como la simulación del IP. La ACL puede aplicarse en interfaces entrantes o salientes en routers.

En las Plataformas que no tienen la opción a utilizar reciba ACL (rACLs), él es posible permitir el tráfico del User Datagram Protocol (UDP) al router de los IP Addresses de confianza con la interfaz ACL.

La lista de acceso ampliada siguiente se puede adaptar a su red. Este ejemplo asume que el router tiene IP Addresses 192.168.10.1 y 172.16.1.1 configurados en sus interfaces, que todo el acceso SNMP debe ser restringido a una estación de administración con la dirección IP de 10.1.1.1, y que la necesidad de la estación de administración comunica solamente con la dirección IP 192.168.10.1:

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

La lista de acceso se debe entonces aplicar a todas las interfaces usando estos comandos configuration:

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

Todos los dispositivos que comunican directamente con el router en los puertos UDP necesitarán ser enumerados específicamente en la lista de acceso antedicha. El Cisco IOS Software utiliza los puertos en el rango 49152 a 65535 como el puerto de origen para las sesiones de salida tales como interrogaciones del Domain Name System (DNS).

Para los dispositivos que tienen muchos IP Addresses configurados, o muchos host que necesiten comunicar con el router, esto puede no ser una solución escalable.

[rACLs](#)

Para las plataformas distribuidas, el rACLs puede ser una opción que comienza en el Cisco IOS Software Release 12.0(21)S2 para las Cisco 12000 Series routers de switch Gigabit (GRS) y liberar 12.0(24)S para las Cisco 7500 Series. Las Listas de acceso de la recepción protegen el dispositivo contra el tráfico dañino antes de que el tráfico pueda afectar el Route Processor. Reciba la trayectoria ACL también se consideran una mejor práctica de la seguridad de la red, y debe ser considerado como una adición a largo plazo a la buena seguridad de la red, así como solución alternativa para esta vulnerabilidad específica. Carga de la CPU se distribuye a los procesadores del linecard y las ayudas atenúan la carga en el procesador del ruta principal. El White Paper titulado [GSR: Reciba las listas de control de acceso](#) ayudará a identificar y a permitir

el tráfico legítimo a su dispositivo y a negar todos los paquetes no deseados.

[ACL de Infraestructura](#)

Aunque sea a menudo difícil bloquear el tráfico que transita su red, es posible identificar el tráfico que se debe nunca permitir apuntar sus dispositivos de infraestructura y bloquear ese tráfico en la frontera de su red. La infraestructura ACL (iACLs) se considera una mejor práctica de la seguridad de la red y se debe considerar como una adición a largo plazo a la buena seguridad de la red así como solución alternativa para esta vulnerabilidad específica. El White Paper titulado [protegiendo su base: Las listas de control de acceso de la Protección de la Infraestructura](#) presentan las guías de consulta y las técnicas recomendadas del despliegue para los iACLs.

[Función de seguridad de Cisco Catalyst LAN Switch](#)

La característica de la lista de IP permitidas restringe el acceso entrante de SNMP y Telnet al switch a direcciones IP de origen no autorizadas. Se admiten mensajes de Syslog y notificaciones de trampa SNMP para notificar a un sistema de administración cuando ocurre una violación o acceso no autorizado.

Una combinación de las funciones de seguridad del Cisco IOS Software se puede utilizar para manejar el Routers y el Switches del Cisco Catalyst. Es necesario establecer una política de seguridad que limite el número de estaciones de administración capaces de acceder a los switches y a los routers.

Para más información sobre cómo aumentar la Seguridad en las redes del IP, refiera a la [seguridad creciente en las redes del IP](#).

[Cómo verificar errores SNMP](#)

Configure la comunidad SNMP ACL con la palabra clave del **registro**. Monitoree el **Syslog** para los intentos fallidos, como demostración abajo.

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

Cuando alguien intenta acceder al router con la comunidad public, usted ve un **Syslog** similar al siguiente:

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

Esta salida significa que la lista de acceso 10 ha negado cinco paquetes snmp del host 172.16.1.1.

Marque periódicamente el SNMP para los errores realizando un **comando show snmp**, como se muestra aquí:

```
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
```

Mire los contadores marcados ****** para los incrementos inesperados en los índices de errores que pueden indicar el intento de explotación de estas vulnerabilidades. Para señalar cualquier problema de seguridad, refiera a la [respuesta a incidente de seguridad de producto de Cisco](#).

Información Relacionada

- [Vulnerabilidades de SNMP de los Cisco Security Advisory](#)
- [V3 de la configuración SNMP con IOS 12.0](#)
- ['Protocolo de administración de red simple \(SNMP\)](#)
- [Configurar el SNMP](#)
- [Soporte Técnico - Cisco Systems](#)