Protocollo SCEP (Simple Network Management Protocol)

Sommario

Introduzione

Questo documento descrive come proteggere il protocollo SNMP (Simple Network Management Protocol).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- SNMP View - Software Cisco IOS® versione 10.3 o successive.
- SNMP versione 3 — Introdotto nel software Cisco IOS versione 12.0(3)T.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Èimportante proteggere il protocollo SNMP soprattutto quando le vulnerabilità del protocollo SNMP possono essere ripetutamente sfruttate per produrre un DoS (Denial of Service).

Strategie per proteggere il protocollo SNMP

Scegliere una stringa della community SNMP valida

Non è buona norma utilizzare le stringhe della community di sola lettura **public** e **private**.

Imposta visualizzazione SNMP

OSPF (Open Shortest Path First) Setup SNMP view Questo comando può bloccare l'utente con accesso limitato a MIB (Management Information Base). Per impostazione predefinita, non è presente SNMP view entry exists . Questo comando è configurato in modalità di configurazione globale e introdotto per la prima volta nel software Cisco IOS versione 10.3. Funziona in modo simile **access-list** in cui se ne SNMP View su alcuni alberi MIB, ogni altro albero è negato inspiegabilmente. Tuttavia, la sequenza non è importante e passa attraverso l'intero elenco per una corrispondenza prima che si fermi.

Per creare o aggiornare una voce di visualizzazione, utilizzare il comando **snmp-server view global configuration** Per rimuovere la voce di visualizzazione del server SNMP specificata, utilizzare il comando **no** forma del comando.

Sintassi:

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

no snmp-server view view-name
```

Descrizione sintassi:

- view-name- Etichetta per il record della vista che viene aggiornato o creato. Il nome viene utilizzato per fare riferimento al record.
- oid-tree - Identificatore oggetto del sottoalbero ASN.1 (Abstract Syntax Notation One) da includere o escludere dalla visualizzazione. Per identificare la sottostruttura, specificare una stringa di testo composta da numeri, ad esempio 1.3.6.2.4, oppure una parola, ad esempio system. Sostituire un singolo identificatore secondario con il carattere jolly asterisco (*) per specificare una famiglia di sottostrutture, ad esempio 1.3.*.4.

- included | excluded- Tipo di vista. È necessario specificare incluso o escluso.

Quando è necessaria una vista, è possibile utilizzare due viste predefinite standard anziché una vista da definire. Uno è tutto, che indica che l'utente può vedere tutti gli oggetti. L'altro è *limitato* , il che indica che l'utente può visualizzare tre gruppi: system, snmpStats,e snmpParties. Le viste predefinite sono descritte nella RFC 1447.

Nota: il primo snmp-server che si immette abilita entrambe le versioni di SNMP.

In questo esempio viene creata una vista che include tutti gli oggetti del gruppo di sistema MIB-II ad eccezione di **sysServices** (Sistema 7) e tutti gli oggetti per l'interfaccia 1 nel gruppo di interfacce MIB-II:

```
snmp-server view agon system included

snmp-server view agon system.7 excluded

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

Questo è un esempio completo di come applicare il MIB con la stringa della community e l'output del snmpwalk con view sul posto. Questa configurazione definisce una visualizzazione che nega l'accesso SNMP alla tabella ARP (Address Resolution Protocol) (atEntry) e lo consente per MIB-II e MIB privato Cisco:

```
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
```

Di seguito viene riportato il comando e l'output per il gruppo di sistema MIB-II:

```
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 %
```

Di seguito viene riportato il comando e l'output per il gruppo di sistema Cisco locale:

```
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
```

Di seguito viene riportato il comando e l'output per la tabella ARP MIB-II:

```
NMSPrompt 84 % snmpwalk cough atTable

no MIB objects contained under subtree.

NMSPrompt 85 %
```

Impostazione della community SNMP con Access-list

Le best practice correnti consigliano di applicare gli Access Control Lists (ACL) alle stringhe della community e di verificare che le stringhe della community delle richieste non siano identiche alle stringhe della community delle notifiche. Gli elenchi degli accessi forniscono un'ulteriore protezione se utilizzati in combinazione con altre misure di protezione.

In questo esempio viene impostato l'ACL sulla stringa della community:

```
access-list 1 permit 10.1.1.1

snmp-server community string1 ro 1
```

Quando si utilizzano stringhe della community diverse per le richieste e i messaggi trap, si riduce la probabilità di ulteriori attacchi o compromessi se la stringa della community viene individuata da un utente non autorizzato. In caso contrario, un utente non autorizzato potrebbe compromettere un dispositivo remoto o intercettare un messaggio trap dalla rete senza autorizzazione.

Una volta abilitata la trap con una stringa della community, la stringa può essere abilitata per l'accesso SNMP in alcuni software Cisco IOS. È necessario disabilitare esplicitamente questa community. Ad esempio:

```
access-list 10 deny any
snmp-server host 10.1.1.1 mystring1
snmp-server community mystring1 RO 10
```

Configurazione di SNMP versione 3

L'SNMP versione 3 è stato introdotto per la prima volta nel software Cisco IOS versione 12.0, ma non è ancora usato comunemente nella gestione della rete. Per configurare il protocollo SNMP versione 3, procedere come segue:

1. Assegnare un ID motore per l'entità SNMP (facoltativo).
2. Definire un utente, **utente** che appartiene al gruppo **group one** e applicare **noAuthentication** (nessuna password) e **noPrivacy** (nessuna crittografia) a questo utente.
3. Definire un utente, **usertwo ;**che appartenga al gruppo **group two** e applicare **noAuthentication** (no password) e **noPrivacy** (no encryption) a questo utente.
4. Definire un utente, **utentetre** che appartiene al gruppo **tre** e applicare all'utente l'**autenticazione** (la password è user3passwd) e la **nonPrivacy** (nessuna crittografia).
5. Definire un utente, **userfour**, che appartenga al gruppo **groupfour** e applicare la **crittografia Authentication** (password è user4passwd) e **Privacy** (des56) a questo utente.
6. Definire un gruppo, **groupone**, tramite User Security Model (USM) V3 e abilitare l'accesso in lettura nella visualizzazione **predefinita v1** (predefinita).
7. Definire un gruppo, il **gruppo due**, mediante USM V3 e abilitare l'accesso in lettura sulla vista **myview**.
8. Definire un gruppo, il **gruppo tre**, tramite USM V3 e abilitare l'accesso in lettura nella visualizzazione **predefinita v1** (predefinita) tramite l'**autenticazione**.
9. Definire un gruppo, il **gruppo quattro**, tramite USM V3 e abilitare l'accesso in lettura nella visualizzazione **predefinita v1** (predefinita), tramite **Autenticazione** e **Privacy**.
10. Definire una vista, **myview**, che fornisce l'accesso in lettura su MIB-II e nega l'accesso in lettura sul MIB Cisco privato.OSPF (Open Shortest Path First) **show running** l'output fornisce righe aggiuntive per il gruppo **public**, perché è stata definita una stringa della community di sola lettura **public**.OSPF (Open Shortest Path First) **show running** l'output non visualizza l'**utente tre**.

Esempio:

```
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
```

Di seguito viene riportato il comando e l'output per il gruppo di sistema MIB-II con **utente** :

```
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 %
```

Questo è il comando e l'output per il gruppo di sistema MIB-II con l'utente **usertwo**:

```
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
```

Di seguito viene riportato il comando e l'output per il Cisco Local System Group con l'utente **user user**:

```
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"
```

Di seguito viene riportato il comando e l'output che mostrano che non è possibile ottenere il gruppo di sistema locale Cisco con l'utente **usertwo**:

```
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 %
```

Questo comando e il risultato finale sono per un tcpdump (patch per supporto SNMP versione 3 e supplemento di 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
```

Configurazione di ACL sulle interfacce

La funzionalità ACL fornisce misure di sicurezza che prevengono attacchi quali lo spoofing IP. L'ACL può essere applicato alle interfacce in entrata o in uscita sui router.

Sulle piattaforme che non possono usare gli ACL di ricezione (rACL), è possibile autorizzare il traffico UDP (User Datagram Protocol) verso il router da indirizzi IP attendibili con ACL di interfaccia.

Il prossimo elenco di accessi esteso può essere adattato alla rete. Nell'esempio si presume che gli indirizzi IP 192.168.10.1 e 172.16.1.1 del router siano configurati sulle interfacce, che l'accesso SNMP sia limitato a una stazione di gestione con indirizzo IP 10.1.1.1 e che la stazione di gestione comunichi solo con l'indirizzo IP 192.168.10.1:

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

OSPF (Open Shortest Path First) access-list deve quindi essere applicato a tutte le interfacce con questi comandi di configurazione:

```
interface ethernet 0/0

ip access-group 101 in
```

Tutti i dispositivi che comunicano direttamente con il router sulle porte UDP devono essere elencati in modo specifico nell'elenco degli accessi precedente. Il software Cisco IOS utilizza le porte da 49152 a 65535 come porta di origine per le sessioni in uscita, ad esempio le query DNS (Domain Name System).

Per i dispositivi con molti indirizzi IP configurati o molti host che devono comunicare con il router, questa non è sempre una soluzione scalabile.

ACL

Per le piattaforme distribuite, gli ACL possono essere un'opzione che inizia nel software Cisco IOS versione 12.0(21)S2 per Cisco serie 12000 Gigabit Switch Router (GSR) e versione 12.0(24)S per Cisco serie 7500. Gli elenchi degli accessi ricevuti proteggono il dispositivo dal traffico dannoso prima che il traffico possa influire sul processore di routing. Anche gli ACL di ricezione dei percorsi sono considerati una best practice per la sicurezza della rete e devono essere considerati un'aggiunta a lungo termine alla buona sicurezza della rete, oltre a una soluzione per questa vulnerabilità specifica. Il carico della CPU viene distribuito ai processori della scheda di linea e contribuisce a ridurre il carico sul processore di routing principale. Il white paper intitolato GSR: receive Access Control List aiuta a identificare il traffico legittimo. Utilizzare questo white paper per

comprendere come inviare traffico legittimo al dispositivo e negare inoltre tutti i pacchetti indesiderati.

ACL di infrastruttura

Sebbene sia spesso difficile bloccare il traffico che attraversa la rete, è possibile identificare il traffico che non deve mai essere autorizzato a raggiungere i dispositivi dell'infrastruttura e bloccare il traffico al confine della rete. Gli ACL di infrastruttura (iACL) sono considerati una best practice per la sicurezza della rete e devono essere considerati un'aggiunta a lungo termine alla buona sicurezza della rete, nonché una soluzione per risolvere questa vulnerabilità specifica. Il white paper, Protecting Your Core: Infrastructure Protection Access Control Lists, presenta le linee guida e le tecniche di implementazione consigliate per gli iACL.

Funzione di sicurezza Cisco Catalyst LAN Switch

La funzionalità dell'elenco di autorizzazioni IP limita l'accesso Telnet e SNMP in entrata allo switch da indirizzi IP di origine non autorizzati. I messaggi Syslog e le trap SNMP sono supportati per notificare a un sistema di gestione il verificarsi di una violazione o di un accesso non autorizzato.

Èpossibile usare una combinazione delle funzionalità di sicurezza del software Cisco IOS per gestire i router e gli switch Cisco Catalyst. È necessario stabilire una policy di sicurezza che limiti il numero di stazioni di gestione che possono accedere agli switch e ai router.

Per ulteriori informazioni su come aumentare la sicurezza sulle reti IP, consultare il documento sull'aumento della sicurezza sulle reti IP.

Come controllare gli errori SNMP

Configurare gli ACL della community SNMP con **log** parola chiave. Monitor (Monitora) **syslog** per i tentativi non riusciti, come mostrato di seguito.

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

Quando qualcuno tenta di accedere al router con il pubblico della community, viene visualizzato un messaggio syslog simile a questo:

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

Questo output indica che access-list 10 ha rifiutato cinque pacchetti SNMP dell'host 172.16.1.1.

Controllare periodicamente SNMP per rilevare eventuali errori con show snmp come mostrato di seguito:

```
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
```

Guarda i contatori contrassegnati con ** per aumenti imprevisti nelle percentuali di errore che possono indicare tentativi di sfruttamento di queste vulnerabilità. Per la segnalazione di problemi relativi alla sicurezza, consultare il documento Cisco sulla risposta ai problemi di sicurezza dei prodotti.

Informazioni correlate

- Vulnerabilità SNMP dei consigli sulla sicurezza di Cisco
- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).