Gestione di mallocfail e di un elevato utilizzo della CPU derivante dal worm "Code Red"

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
In che modo il worm "Code Red" infetta altri sistemi
Consigli che parlano del worm "Code Red"
Sintomi
Identificare il dispositivo infetto
Tecniche di prevenzione
Blocca traffico sulla porta 80
Riduzione dell'utilizzo della memoria di input ARP
Usa switching Cisco Express Forwarding (CEF)
Cisco Express Forwarding e Fast Switching
Comportamento e implicazioni della commutazione rapida
Vantaggi del CEF
Output di esempio: CEF
Fattori da considerare
"Code Red" Domande frequenti e relative risposte
D. Uso NAT e utilizzo al 100% la CPU nell'input IP. Quando si esegue il comando show proc cpu, l'utilizzo della CPU è elevato in livello di interrupt - 100/99 o 99/98. Ciò è correlato a "Code Red"?
D. Il processo di input di HyBridge richiede un elevato utilizzo della CPU. Perché questo accade? È collegato a "Code Red"?
D. L'utilizzo della CPU è elevato a livello di interrupt e si ricevono scaricamenti se si prova a visualizzare il registro. Anche il traffico è solo leggermente superiore al normale. Qual è la ragione di questo?
D. Sono visibili numerosi tentativi di connessione HTTP sul router IOS che esegue un http-server ip. E' per via della scansione dei vermi "Code Red"?
Soluzioni
Informazioni correlate

Introduzione

Questo documento descrive il worm "Code Red" e i problemi che il worm può causare in un ambiente di routing Cisco. Questo documento descrive anche le tecniche per prevenire l'infestazione del verme e fornisce i collegamenti agli advisory correlati che descrivono le soluzioni per i problemi relativi al verme.

Il worm "Code Red" sfrutta una vulnerabilità nel servizio di indicizzazione di Microsoft Internet Information Server (IIS) versione 5.0. Quando il worm "Code Red" infetta un host, provoca il probe dell'host e l'infezione di una serie casuale di indirizzi IP, causando un netto aumento del traffico di rete. Questo è particolarmente problematico se vi sono collegamenti ridondanti nella rete e/o se Cisco Express Forwarding (CEF) non viene utilizzato per commutare i pacchetti.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

In che modo il worm "Code Red" infetta altri sistemi

Il worm "Code Red" tenta di connettersi a indirizzi IP generati in modo casuale. Ogni server IIS infetto può tentare di infettare lo stesso gruppo di dispositivi. È possibile tracciare l'indirizzo IP di origine e la porta TCP del worm perché non è oggetto di spoofing. L'URPF (Unicast Reverse Path Forwarding) non può eliminare un attacco worm perché l'indirizzo di origine è valido.

Consigli che parlano del worm "Code Red"

Questi consigli descrivono il worm "Code Red" e spiegano come applicare patch al software interessato dal worm:

- Cisco Security Advisory: Worm "rosso codice" - Impatto sul cliente
- Overflow del buffer dell'estensione ISAPI del server indice IIS remoto
- .ida "Code Red" Worm
- CERTIFICATO? Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL

Sintomi

Di seguito sono riportati alcuni sintomi che indicano che un router Cisco è interessato dal worm

"Code Red":

- Numero elevato di flussi nelle tabelle NAT o PAT (se si utilizza NAT o PAT).
- Numerose richieste ARP o tempeste ARP nella rete (causate dalla scansione dell'indirizzo IP).
- Utilizzo eccessivo di memoria da parte dei processi IP Input, ARP Input, IP Cache Ager e CEF.
- Elevato utilizzo della CPU in ARP, IP Input, CEF e IPC.
- Utilizzo elevato della CPU a livello di interrupt a bassa velocità di traffico o utilizzo elevato della CPU a livello di processo in input IP, se si utilizza NAT.

Una condizione di memoria insufficiente o un elevato utilizzo sostenuto della CPU (100%) a livello di interrupt può causare il ricaricamento di un router Cisco IOS®. Il ricaricamento è causato da un processo che si comporta in modo errato a causa delle condizioni di stress.

Se non si ha il sospetto che i dispositivi del sito siano infettati dal worm "Code Red" o ne siano la destinazione, consultare la sezione Informazioni correlate per ulteriori URL su come risolvere i problemi.

Identificare il dispositivo infetto

Usare la commutazione di flusso per identificare l'indirizzo IP di origine del dispositivo interessato. Configurare il **flusso ip route-cache** su tutte le interfacce per registrare tutti i flussi commutati dal router.

Dopo alcuni minuti, eseguire il comando **show ip cache flow** per visualizzare le voci registrate. Durante la fase iniziale dell'infezione da worm "Code Red", il worm tenta di replicarsi da solo. La replica viene eseguita quando il worm invia richieste HT a indirizzi IP casuali. Pertanto, è necessario cercare le voci di flusso della cache con la porta di destinazione 80 (HT., 0050 in formato esadecimale).

Flusso della **cache show ip | include 0050** visualizza tutte le voci della cache con una porta TCP 80 (0050 in formato esadecimale):

```
Router#show ip cache flow | include 0050
...

scram        scrappers    dative      DstIPaddress   Pr SrcP  DstP  Pkts
Vl1       193.23.45.35      Vl3        2.34.56.12    06 0F9F  0050     2
Vl1    211.101.189.208     Null     158.36.179.59    06 0457  0050     1
Vl1       193.23.45.35      Vl3     34.56.233.233    06 3000  0050     1
Vl1     61.146.138.212     Null     158.36.175.45    06 B301  0050     1
Vl1       193.23.45.35      Vl3     98.64.167.174    06 0EED  0050     1
Vl1     202.96.242.110     Null     158.36.171.82    06 0E71  0050     1
Vl1       193.23.45.35      Vl3     123.231.23.45    06 121F  0050     1
Vl1       193.23.45.35      Vl3       9.54.33.121    06 1000  0050     1
Vl1       193.23.45.35      Vl3      78.124.65.32    06 09B6  0050     1
Vl1      24.180.26.253     Null    158.36.179.166    06 1132  0050     1
```

Se si riscontra un numero insolitamente elevato di voci con lo stesso indirizzo IP di origine, indirizzo IP di destinazione casuale[1], DstP = 0050 (HTTP) e Pr = 06 (TCP), è probabile che sia stato individuato un dispositivo infetto. Nell'esempio di output, l'indirizzo IP di origine è 193.23.45.35 e proviene dalla VLAN1.

[1]Un'altra versione del worm "Code Red", chiamata "Code Red II", non sceglie un indirizzo IP di

destinazione totalmente casuale. Al contrario, "Code Red II" mantiene la porzione di rete dell'indirizzo IP e sceglie una porzione host casuale dell'indirizzo IP per propagarsi. Ciò consente al worm di diffondersi più rapidamente all'interno della stessa rete.

"Code Red II " utilizza queste reti e maschere:

```
Mask          Probability of Infection
0.0.0.0         12.5% (random)
255.0.0.0       50.0% (same class A)
255.255.0.0     37.5% (same class B)
```

Gli indirizzi IP di destinazione esclusi sono 127.X.X.X e 224.X.X.X e nessun ottetto può essere 0 o 255. Inoltre, l'host non tenta di infettarsi nuovamente.

Per ulteriori informazioni, fare riferimento al codice rosso (II) .

A volte non è possibile eseguire netflow per rilevare un tentativo di infestazione da "Code Red". Ciò si può verificare perché si esegue una versione del codice che non supporta netflow oppure perché la memoria del router è insufficiente o eccessivamente frammentata per abilitare netflow. Cisco consiglia di non abilitare netflow quando ci sono più interfacce in entrata e solo un'interfaccia in uscita sul router, perché l'accounting netflow viene eseguito sul percorso in entrata. In questo caso, è meglio abilitare l'accounting IP sull'interfaccia di uscita singola.

Nota: il comando ip accounting disabilita il protocollo DCEF. Non abilitare l'accounting IP su piattaforme in cui si desidera utilizzare la commutazione DCEF.

```
Router(config)#interface vlan 1000
Router(config-if)#ip accounting

Router#show ip accounting
  Source            Destination           Packets               Bytes
20.1.145.49     75.246.253.88               2                  96
20.1.145.43     17.152.178.57               1                  48
20.1.145.49     20.1.49.132                 1                  48
20.1.104.194    169.187.190.170             2                  96
20.1.196.207    20.1.1.11                   3                 213
20.1.145.43     43.129.220.118              1                  48
20.1.25.73      43.209.226.231              1                  48
20.1.104.194    169.45.103.230              2                  96
20.1.25.73      223.179.8.154               2                  96
20.1.104.194    169.85.92.164               2                  96
20.1.81.88      20.1.1.11                   3                 204
20.1.104.194    169.252.106.60              2                  96
20.1.145.43     126.60.86.19                2                  96
20.1.145.49     43.134.116.199              2                  96
20.1.104.194    169.234.36.102              2                  96
20.1.145.49     15.159.146.29               2                  96
```

Nell'output del comando show ip accounting cercare gli indirizzi di origine che tentano di inviare pacchetti a più indirizzi di destinazione. Se l'host infetto è in fase di scansione, cerca di stabilire connessioni HTTP ad altri router. Vedrete quindi i tentativi di raggiungere più indirizzi IP. La maggior parte dei tentativi di connessione in genere non riesce. Pertanto, è possibile vedere solo un numero ridotto di pacchetti trasferiti, ciascuno con un numero ridotto di byte. Nell'esempio, è probabile che siano infetti 20.1.145.49 e 20.1.104.194.

Quando si esegue MLS (Multi-Layer Switching) su Catalyst serie 5000 e Catalyst serie 6000, è

necessario eseguire diversi passaggi per abilitare l'accounting netflow e individuare l'infestazione. In uno switch Cat6000 con Supervisor 1 Multilayer Switch Feature Card (MSFC1) o SUP I/MSFC2, il protocollo MLS basato su netflow è abilitato per impostazione predefinita, ma la modalità flusso è solo destinazione. Pertanto, l'indirizzo IP di origine non viene memorizzato nella cache. È possibile abilitare la modalità "full-flow" per rintracciare gli host infetti con l'aiuto del comando **set mls flow full** sul supervisor.

Per la modalità ibrida, usare il comando **set mls flow full**:

```
6500-sup(enable)set mls flow full
Configured IP flowmask is set to full flow.
Warning: Configuring more specific flow mask may dramatically
increase the number of MLS entries.
```

Per la modalità IOS nativa, usare il comando **mls flow ip full**:

```
Router(config)#mls flow ip full
```

Quando si abilita la modalità "flusso completo", viene visualizzato un avviso per indicare un aumento significativo delle voci MLS. L'impatto dell'aumento delle voci MLS è giustificabile per un breve periodo se la rete è già infestata dal worm "Code Red". Il worm causa un aumento e un numero eccessivo di voci MLS.

Per visualizzare le informazioni raccolte, utilizzare i seguenti comandi:

Per la modalità ibrida, usare il comando **set mls flow full**:

```
6500-sup(enable)set mls flow full
Configured IP flowmask is set to full flow.
Warning: Configuring more specific flow mask may dramatically
increase the number of MLS entries.
```

Per la modalità IOS nativa, usare il comando **mls flow ip full**:

```
Router(config)#mls flow ip full
```

Quando si abilita la modalità "flusso completo", viene visualizzato un avviso per indicare un aumento significativo delle voci MLS. L'impatto dell'aumento delle voci MLS è giustificabile per un breve periodo se la rete è già infestata dal worm "Code Red". Il worm causa un aumento e un numero eccessivo di voci MLS.

Per visualizzare le informazioni raccolte, utilizzare i seguenti comandi:

Per la modalità ibrida, usare il comando **show mls ent**:

```
6500-sup(enable)show mls ent
Destination-IP  Source-IP     Prot  DstPrt SrcPrt Destination-Mac   Vlan EDst
ESrc DPort     SPort     Stat-Pkts  Stat-Bytes  Uptime   Age
-------------- --------------- ----- ------ ------ ----------------- ---- ----
---- --------- --------- ---------- ----------- -------- --------
```

Nota: tutti questi campi vengono compilati quando sono in modalità "flusso completo".

Per la modalità IOS nativa, usare il comando **show mls ip**:

```
Router#show mls ip
DstIP           SrcIP           Prot:SrcPort:DstPort  Dst i/f:DstMAC
---------------------------------------------------------------------
Pkts         Bytes       SrcDstPorts    SrcDstEncap Age   LastSeen
---------------------------------------------------------------------
```

Quando si determinano l'indirizzo IP di origine e la porta di destinazione coinvolti nell'attacco, è possibile impostare MLS di nuovo sulla modalità "solo destinazione".

Per la modalità ibrida, usare il comando **set mls flow destination**:

```
6500-sup(enable) set mls flow destination
Usage: set mls flow <destination|destination-source|full>
```

Per la modalità IOS nativa, usare il comando **mls flow ip destination**:

```
Router(config)#mls flow ip destination
```

La combinazione Supervisor (SUP) II/MSFC2 è protetta da attacchi perché la commutazione CEF viene eseguita nell'hardware e vengono mantenute le statistiche netflow. Pertanto, anche durante un attacco "Code Red", se si abilita la modalità di flusso completo, il router non viene sovraccaricato, a causa del meccanismo di commutazione più veloce. I comandi per abilitare la modalità flusso completo e visualizzare le statistiche sono gli stessi su SUP I/MFSC1 e SUP II/MSFC2.

Tecniche di prevenzione

Utilizzare le tecniche elencate in questa sezione per ridurre al minimo l'impatto del worm "Code Red" sul router.

Blocca traffico sulla porta 80

Se è possibile nella rete, il modo più semplice per prevenire l'attacco "Code Red" è bloccare tutto il traffico verso la porta 80, che è la porta più nota per WWW. Creare un elenco degli accessi per negare i pacchetti IP destinati alla porta 80 e applicarlo ai pacchetti in entrata sull'interfaccia interessata dall'origine dell'infezione.

Riduzione dell'utilizzo della memoria di input ARP

L'ingresso ARP utilizza una grande quantità di memoria quando un percorso statico punta a un'interfaccia di broadcast, come questa:

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

Ogni pacchetto per il percorso predefinito viene inviato alla VLAN3. Tuttavia, non è specificato alcun indirizzo IP dell'hop successivo, quindi il router invia una richiesta ARP per l'indirizzo IP di destinazione. Il router dell'hop successivo per la destinazione risponde con il proprio indirizzo MAC, a meno che il proxy ARP non sia disabilitato. La risposta del router crea una voce aggiuntiva nella tabella ARP in cui l'indirizzo IP di destinazione del pacchetto viene mappato

all'indirizzo MAC dell'hop successivo. Il worm "Code Red" invia i pacchetti a indirizzi IP casuali, aggiungendo una nuova voce ARP per ciascun indirizzo di destinazione casuale. Ogni nuova voce ARP consuma una quantità sempre maggiore di memoria nel processo di input ARP.

Non creare un percorso statico predefinito verso un'interfaccia, in particolare se l'interfaccia è broadcast (Ethernet/Fast Ethernet/GE/SMDS) o multipunto (Frame Relay/ATM). Ogni route statica predefinita deve puntare all'indirizzo IP del router dell'hop successivo. Dopo aver modificato il percorso predefinito in modo che punti all'indirizzo IP dell'hop successivo, utilizzare il comando **clear arp-cache** per cancellare tutte le voci ARP. Questo comando risolve il problema di utilizzo della memoria.

Usa switching Cisco Express Forwarding (CEF)

Per ridurre l'utilizzo della CPU su un router IOS, passare dalla commutazione Fast/Optimum/Netflow alla commutazione CEF. Esistono alcune avvertenze per abilitare il CEF. La sezione successiva tratta la differenza tra il CEF e l'opzione di commutazione veloce e spiega le implicazioni quando si abilita il CEF.

Cisco Express Forwarding e Fast Switching

Abilitare CEF per alleviare l'aumento del carico del traffico causato dal worm "Code Red". Il software Cisco IOS® versione 11.1( )CC, 12.0 e successive supportano CEF sulle piattaforme Cisco 7200/7500/GSR. Il supporto per CEF su altre piattaforme è disponibile nel software Cisco IOS versione 12.0 o successive. È possibile eseguire ulteriori ricerche con lo strumento Software Advisor.

A volte, non è possibile abilitare il protocollo CEF su tutti i router per uno dei motivi seguenti:

- Memoria insufficiente
- Architetture di piattaforma non supportate
- Incapsulamenti di interfaccia non supportati

Comportamento e implicazioni della commutazione rapida

Di seguito sono riportate le implicazioni dell'utilizzo dell'opzione di commutazione veloce:

- Cache basata sul traffico: la cache è vuota finché il router non cambia i pacchetti e li popola.
- Primo pacchetto con commutazione di contesto: il primo pacchetto viene commutato di contesto, in quanto la cache è inizialmente vuota.
- Cache granulare: la cache viene creata in base alla granularità della voce RIB (Routing Information Base) più specifica di una rete principale. Se RIB ha /24s per la rete principale 131.108.0.0, la cache viene creata con /24s per questa rete principale.
- /32 viene utilizzata la cache—/32 viene utilizzata per bilanciare il carico per ogni destinazione. Quando la cache esegue il bilanciamento del carico, viene creata con /32s per la rete principale.**Nota:** questi ultimi due problemi possono potenzialmente causare una cache di grandi dimensioni che consumerebbe tutta la memoria.
- Memorizzazione nella cache ai limiti della rete principale: con l'instradamento predefinito, la memorizzazione nella cache viene eseguita ai limiti della rete principale.
- Ager cache: l'agente cache viene eseguito ogni minuto e controlla 1/20 (5%) della cache per

individuare le voci inutilizzate in condizioni di memoria normali e 1/4 (25%) della cache in condizioni di memoria insufficiente (200 k).

Per modificare i valori indicati, usare il comando **ip cache-ager-interval X Y Z**, dove:

- X è <0-2147483> il numero di secondi tra un'esecuzione dello strumento di gestione e l'altra. Impostazione predefinita = 60 secondi.
- Y è <2-50> 1/(Y+1) di cache da aggiornare per esecuzione (memoria insufficiente). Impostazione predefinita = 4.
- Z è <3-100> 1/(Z+1) di cache per durata per esecuzione (normale). Impostazione predefinita = 20.

Di seguito è riportata una configurazione di esempio che utilizza **ip cache-ager 60 5 25**.

```
Router#show ip cache
IP routing cache 2 entries, 332 bytes
   27 adds, 25 invalidates, 0 refcounts
Cache aged by 1/25 every 60 seconds (1/5 when memory is low).
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 03:55:12 ago

Prefix/Length          Age    Interface     Next Hop
4.4.4.1/32        03:44:53    Serial1       4.4.4.1
192.168.9.0/24    00:03:15    Ethernet1    20.4.4.1

Router#show ip cache verbose
IP routing cache 2 entries, 332 bytes
   27 adds, 25 invalidates, 0 refcounts
Cache aged by 1/25 every 60 seconds (1/5 when memory is low).
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 03:57:31 ago
Prefix/Length       Age       Interface       Next Hop
4.4.4.1/32-24           03:47:13  Serial1         4.4.4.1
                    4   0F000800
192.168.9.0/24-0        00:05:35  Ethernet1       20.4.4.1
                    14  00000C34A7FC00000C13DBA90800
```

In base all'impostazione del gestore della cache, una percentuale delle voci della cache non rientra nella tabella della cache veloce. Quando le voci scadono rapidamente, una percentuale maggiore della tabella cache veloce invecchia e la tabella cache diventa più piccola. Di conseguenza, il consumo di memoria sul router si riduce. Uno svantaggio è rappresentato dal continuo flusso del traffico per le voci obsolete al di fuori della tabella della cache. I pacchetti iniziali sono commutati in base al processo, il che provoca un breve picco nell'utilizzo della CPU nell'**input IP** fino a quando non viene creata una nuova voce della cache per il flusso.

Dal software Cisco IOS versione 10.3(8), 11.0(3) e successive, lo strumento di gestione della cache IP viene gestito in modo diverso, come spiegato di seguito:

- i comandi **ip cache-ager-interval** e **ip cache-invalidate-delay** sono disponibili solo se il comando **service internal** è definito nella configurazione.
- Se il periodo tra le esecuzioni dell'annullamento della convalida dell'ager è impostato su 0, il processo dell'ager viene completamente disabilitato.
- Il tempo è espresso in secondi.

Nota: quando si eseguono questi comandi, l'utilizzo della CPU del router aumenta. Utilizzare questi comandi solo quando assolutamente necessario.

```
Router#clear ip cache ?
A.B.C.D Address prefix
<CR>--> will clear the entire cache and free the memory used by it!

Router#debug ip cache
IP cache debugging is on
```

Vantaggi del CEF

- La tabella FIB (Forwarding Information Base) viene creata in base alla tabella di routing. Pertanto, le informazioni di inoltro esistono prima dell'inoltro del primo pacchetto. Il FIB contiene inoltre le voci /32 per gli host LAN connessi direttamente.
- La tabella Adiacente (ADJ) contiene le informazioni di riscrittura di layer 2 per gli hop successivi e gli host connessi direttamente (una voce ARP crea una adiacenza CEF).
- Non esiste un concetto di cache ager con CEF per aumentare l'utilizzo della CPU. Una voce FIB viene eliminata se viene eliminata una voce della tabella di routing.

Attenzione: anche in questo caso, un percorso predefinito che punta a un'interfaccia broadcast o multipunto indica che il router invia richieste ARP per ogni nuova destinazione. Le richieste ARP provenienti dal router potrebbero creare una tabella adiacente enorme finché il router non esaurisce la memoria. Se il CEF non riesce ad allocare memoria, il CEF/DCEF si disattiva da solo. Sarà necessario riattivare manualmente CEF/DCEF.

Output di esempio: CEF

Di seguito viene riportato un output di esempio del comando show ip cef summary che mostra l'utilizzo della memoria. Questo output viene generato come istantanea di un server di routing Cisco 7200 con software Cisco IOS versione 12.0.

```
Router>show ip cef summary
IP CEF with switching (Table Version 2620746)
  109212 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 84625
  109212 leaves, 8000 nodes, 22299136 bytes, 2620745 inserts, 2511533
  invalidations
  17 load sharing elements, 5712 bytes, 109202 references
  universal per-destination load sharing algorithm, id 6886D006
  1 CEF resets, 1 revisions of existing leaves
  1 in-place/0 aborted modifications
  Resolution Timer: Exponential (currently 1s, peak 16s)
  refcounts:  2258679 leaf, 2048256 node

Adjacency Table has 16 adjacencies


Router>show processes memory | include CEF
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
  73   0     147300       1700     146708          0          0 CEF process
  84   0        608          0       7404          0          0 CEF Scanner


Router>show processes memory | include BGP

   2   0    6891444    6891444       6864          0          0 BGP Open
```

```
  80   0       3444       2296       8028          0          0 BGP Open
  86   0     477568     476420       7944          0          0 BGP Open
  87   0 2969013892  102734200  338145696          0          0 BGP Router
  88   0   56693560 2517286276       7440     131160    4954624 BGP I/O
  89   0      69280   68633812      75308          0          0 BGP Scanner
  91   0    6564264    6564264       6876          0          0 BGP Open
 101   0    7635944    7633052       6796        780          0 BGP Open
 104   0    7591724    7591724       6796          0          0 BGP Open
 105   0    7269732    7266840       6796        780          0 BGP Open
 109   0    7600908    7600908       6796          0          0 BGP Open
 110   0    7268584    7265692       6796        780          0 BGP Open
```

```
Router>show memory summary | include FIB

Alloc PC        Size     Blocks      Bytes    What
0x60B8821C       448          7       3136    FIB: FIBIDB
0x60B88610     12000          1      12000    FIB: HWIDB MAP TABLE
0x60B88780       472          6       2832    FIB: FIBHWIDB
0x60B88780       508          1        508    FIB: FIBHWIDB
0x60B8CF9C      1904          1       1904    FIB 1 path chunk pool
0x60B8CF9C     65540          1      65540    FIB 1 path chunk pool
0x60BAC004      1904        252     479808    FIB 1 path chun
0x60BAC004     65540        252   16516080    FIB 1 path chun
```

```
Router>show memory summary | include CEF

0x60B8CD84      4884          1       4884    CEF traffic info
0x60B8CF7C        44          1         44    CEF process
0x60B9D12C     14084          1      14084    CEF arp throttle chunk
0x60B9D158       828          1        828    CEF loadinfo chunk
0x60B9D158     65540          1      65540    CEF loadinfo chunk
0x60B9D180       128          1        128    CEF walker chunk
0x60B9D180       368          1        368    CEF walker chunk
0x60BA139C        24          5        120    CEF process
0x60BA139C        40          1         40    CEF process
0x60BA13A8        24          4         96    CEF process
0x60BA13A8        40          1         40    CEF process
0x60BA13A8        72          1         72    CEF process
0x60BA245C        80          1         80    CEF process
0x60BA2468        60          1         60    CEF process
0x60BA65A8     65488          1      65488    CEF up event chunk
```

```
Router>show memory summary | include adj

0x60B9F6C0       280          1        280    NULL adjacency
0x60B9F734       280          1        280    PUNT adjacency
0x60B9F7A4       280          1        280    DROP adjacency
0x60B9F814       280          1        280    Glean adjacency
0x60B9F884       280          1        280    Discard adjacency
0x60B9F9F8     65488          1      65488    Protocol adjacency chunk
```

Fattori da considerare

Quando il numero di flussi è elevato, CEF in genere consuma meno memoria rispetto all'opzione di commutazione veloce. Se la memoria è già utilizzata da una cache a commutazione rapida, è necessario cancellare la cache ARP (tramite il comando **clear ip arp**) prima di abilitare CEF.

Nota: quando si cancella la cache, si verifica un picco nell'utilizzo della CPU del router.

"Code Red" Domande frequenti e relative risposte

D. Uso NAT e utilizzo al 100% la CPU nell'input IP. Quando si esegue il comando show proc cpu, l'utilizzo della CPU è elevato in livello di interrupt - 100/99 o 99/98. Ciò è correlato a "Code Red"?

R. È stato recentemente risolto un bug NAT Cisco (CSCdu63623 (solo utenti registrati)) che implica la scalabilità. Quando sono presenti decine di migliaia di flussi NAT (in base al tipo di piattaforma), il bug causa un utilizzo al 100% della CPU a livello di processo o di interrupt.

Per stabilire se il bug è stato causato, usare il comando **show align** e verificare se il router è in grado di rilevare errori di allineamento. Se vengono rilevati errori di allineamento o accessi alla memoria spurie, usare il comando **show align** un paio di volte per verificare se gli errori sono in aumento. Se il numero di errori è in aumento, gli errori di allineamento possono essere la causa di un elevato utilizzo della CPU a livello di interrupt e non il bug Cisco CSCdu63623 (solo utenti registrati). Per ulteriori informazioni, consultare il documento sulla risoluzione dei problemi di allineamento e di accessi spuri.

Per visualizzare il numero di traduzioni attive, usare il comando **show ip nat translation**. Il punto di fusione per un processore di classe NPE-300 è di circa 20.000-40.000 traduzioni. Questo numero varia in base alla piattaforma in uso.

Questo problema di fusione è stato osservato in precedenza da un paio di clienti, ma dopo "Code Red", più clienti hanno sperimentato questo problema. L'unica soluzione è eseguire NAT (anziché PAT), in modo da ridurre il numero di traduzioni attive. Se si dispone di un 7200, utilizzare un NSE-1 e ridurre i valori di timeout NAT.

D. Il processo di input di HyBridge richiede un elevato utilizzo della CPU. Perché questo accade? È collegato a "Code Red"?

R. Il processo di input HyBridge gestisce tutti i pacchetti che non possono essere commutati rapidamente dal processo IRB. L'incapacità del processo IRB di commutare rapidamente un pacchetto può essere causata da:

- Il pacchetto è un pacchetto di trasmissione.
- Il pacchetto è multicast.
- Destinazione sconosciuta. È necessario attivare ARP.
- Sono presenti BPDU Spanning Tree.

HyBridge Input incontra problemi se ci sono migliaia di interfacce point-to-point nello stesso gruppo di bridge. HyBridge Input rileva anche dei problemi (ma in misura minore) se ci sono migliaia di VS nella stessa interfaccia multipunto.

Quali sono le possibili cause dei problemi con IRB? Si supponga che un dispositivo infettato da "Code red" esegua la scansione degli indirizzi IP.

- Il router deve inviare una richiesta ARP per ciascun indirizzo IP di destinazione. Per ogni indirizzo analizzato, su ogni VC del gruppo bridge viene generata una quantità di richieste ARP. Il normale processo ARP non causa problemi alla CPU. Tuttavia, se esiste una voce ARP senza una voce bridge, il router inoltra i pacchetti destinati a indirizzi per cui esistono già voci ARP. Ciò può causare un elevato utilizzo della CPU poiché il traffico è commutato in

base al processo. Per evitare il problema, aumentare il tempo di invecchiamento del bridge (per impostazione predefinita 300 secondi o 5 minuti) in modo che corrisponda o superi il timeout ARP (per impostazione predefinita 4 ore) in modo che i due timer siano sincronizzati.
- L'indirizzo che l'host finale tenta di infettare è un indirizzo di broadcast. Il router esegue l'equivalente di una trasmissione subnet che deve essere replicata dal processo di input HyBridge. Questo non accade se il comando **no ip direct-broadcast** è configurato. Dal software Cisco IOS versione 12.0, il comando **ip direct-broadcast** è disabilitato per impostazione predefinita, ossia tutte le trasmissioni dirette dall'IP vengono eliminate.
- Di seguito è riportata una nota rapida, non correlata a "Code Red" e correlata alle architetture IRB:Ènecessario replicare i pacchetti multicast e broadcast di layer 2. Pertanto, un problema con i server IPX in esecuzione su un segmento di broadcast può determinare l'interruzione del collegamento. È possibile utilizzare i criteri di sottoscrizione per evitare il problema. Per ulteriori informazioni, fare riferimento al supporto bridge xDSL (x Digital Subscriber Line). Inoltre, è necessario considerare gli elenchi degli accessi bridge, che limitano il tipo di traffico autorizzato a passare attraverso il router.
- Per risolvere questo problema IRB, è possibile utilizzare più gruppi di bridge e verificare che esista un mapping uno-a-uno per BVI, sottointerfacce e VC.
- L'RBE è superiore all'IRB perché evita del tutto lo stack di bridging. È possibile eseguire la migrazione a RBE da IRB. I seguenti bug Cisco ispirano tale migrazione:CSCdr1146 (solo utenti registrati)CSCdp18572 (solo utenti registrati)CSCds40806 (solo utenti registrati)

D. L'utilizzo della CPU è elevato a livello di interrupt e si ricevono scaricamenti se si prova a visualizzare il registro. Anche il traffico è solo leggermente superiore al normale. Qual è la ragione di questo?

A. Di seguito è riportato un esempio dell'output del comando **show logging**:

```
Router#show logging
     Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
                                                ^
                                              this value is non-zero
         Console logging: level debugging, 9 messages logged
```

Controllare se si accede alla console. In caso affermativo, verificare se sono presenti richieste HTTP relative al traffico. Quindi, controllare se ci sono elenchi degli accessi con parole chiave o debug che guardano particolari flussi IP. In caso di aumento degli svuotamenti, è possibile che la console, in genere una periferica a 9600 baud, non sia in grado di gestire la quantità di informazioni ricevute. In questo scenario, il router disabilita gli interrupt ed elabora solo i messaggi della console. La soluzione consiste nel disattivare la registrazione sulla console o nel rimuovere qualsiasi tipo di registrazione eseguita.

D. Sono visibili numerosi tentativi di connessione HTTP sul router IOS che esegue un http-server ip. E' per via della scansione dei vermi "Code Red"?

R."Codice rosso" può essere il motivo qui. Cisco consiglia di disabilitare il comando **ip http server** sul router IOS in modo che non debba gestire numerosi tentativi di connessione da host infetti.

Soluzioni

Sono disponibili diverse soluzioni alternative illustrate nella sezione Consigli che trattano il worm "Code Red". Per le soluzioni alternative, consultare le avvertenze.

Un altro metodo per bloccare il worm "Code Red" sui punti di ingresso della rete è tramite l'uso di NBAR (Network-Based Application Recognition) e ACL (Access Control Lists) all'interno del software IOS sui router Cisco. Utilizzare questo metodo insieme alle patch consigliate per i server IIS di Microsoft. Per ulteriori informazioni su questo metodo, consultare il documento sull'uso di NBAR e ACL per bloccare il worm "Code Red" sui punti di ingresso della rete.

Informazioni correlate

- Risoluzione dei problemi relativi alla memoria
- Risoluzione dei problemi di perdita dei buffer
- Risoluzione dei problemi relativi all'utilizzo elevato della CPU nei router Cisco
- Risoluzione dei problemi di blocco del router
- Note tecniche sulla risoluzione dei problemi - Router
- Risoluzione dei problemi del router
- Documentazione e supporto tecnico – Cisco Systems