Lidando com mallocfail e utilização elevada de CPU, resultante do worm "código vermelho”

Contents

Introduction

Este documento descreve o worm “Code Red” e os problemas que ele pode causar em um ambiente de roteamento Cisco. Este documento também descreve técnicas para evitar infestação do worm e fornece links para as recomendações relacionadas que descrevem soluções para problemas relacionados ao worm.

O worm "Code Red" explora uma vulnerabilidade no Serviço de Índice do Microsoft Internet Information Server (IIS) versão 5.0. Quando o worm "Code Red" infecta um host, ele faz com que o host investigue e infecte uma série aleatória de endereços IP, o que causa um aumento acentuado no tráfego de rede. Isso é especialmente problemático se houver links redundantes na rede e/ou se o Cisco Express Forwarding (CEF) não for usado para comutar pacotes.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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, make sure that you understand the potential impact of any command.

Conventions

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

Como o worm "Code Red" infecta outros sistemas

O worm "Código Vermelho" tenta se conectar a endereços IP gerados aleatoriamente. Cada servidor IIS infectado pode tentar infectar o mesmo conjunto de dispositivos. Você pode rastrear o endereço IP origem e a porta TCP do worm porque ele não está falsificado. O Unicast Reverse Path Forwarding (URPF) não pode suprimir um ataque de worm porque o endereço de origem é legal.

Consultivos que discutem o worm "Código Vermelho"

Essas recomendações descrevem o worm "Code Red" e explicam como corrigir o software afetado pelo worm:

- Consultivo de segurança Cisco: Worm "código vermelho" - impacto para o cliente
- Excesso de buffer do Index Server ISAPI Extension de IIS remoto
- Worm .ida "código vermelho"
- CERT? Aconselhamento CA-2001-19 Worm "Code Red" Explorando Estouro de Buffer na DLL do Serviço de Indexação IIS

Sintomas

Estes são alguns sintomas que indicam que um roteador Cisco é afetado pelo worm "Code Red":

- Grande número de fluxos em tabelas NAT ou PAT (se você usar NAT ou PAT).
- Grande número de solicitações ARP ou tempestades ARP na rede (causadas pela verificação de endereço IP).
- Uso excessivo de memória por IP Input, ARP Input, IP Cache Ager e processos CEF.
- Alta utilização da CPU em ARP, IP Input, CEF e IPC.
- Alta utilização da CPU no nível de interrupção a baixas taxas de tráfego ou alta utilização da CPU no nível do processo na entrada IP, se você usar NAT.

Uma condição de memória baixa ou alta utilização sustentada da CPU (100%) no nível de interrupção pode fazer com que um roteador Cisco IOS® seja recarregado. A recarga é causada por um processo que se comporta incorretamente devido às condições de estresse.

Se você não suspeitar que os dispositivos no seu site estão infectados pelo worm "Code Red" ou são o alvo do mesmo, consulte a seção Informações Relacionadas para obter URLs adicionais sobre como solucionar qualquer problema encontrado.

Identificar o dispositivo infectado

Use a comutação de fluxo para identificar o endereço IP de origem do dispositivo afetado. Configure o fluxo do cache de rota IP em todas as interfaces para registrar todos os fluxos comutados pelo roteador.

Após alguns minutos, emita o comando show ip cache flow para ver as entradas gravadas. Durante a fase inicial da infecção do worm "Código Vermelho", o worm tenta se replicar. A replicação ocorre quando o worm envia solicitações HT a endereços IP aleatórios. Portanto, você deve procurar entradas de fluxo de cache com a porta de destino 80 (HT., 0050 em hexadecimal).

O **show ip cache flow | include 0050** exibe todas as entradas de cache com uma porta TCP 80 (0050 em hexadecimal):

```
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 você encontrar um número anormalmente alto de entradas com o mesmo endereço IP de origem, endereço IP de destino aleatório [1], DstP = 0050 (HTTP) e Pr = 06 (TCP), você provavelmente localizou um dispositivo infectado. Neste exemplo de saída, o endereço IP origem é 193.23.45.35 e vem da VLAN1.

[1] Outra versão do worm "Code Red", chamada "Code Red II", não escolhe um endereço IP de destino totalmente aleatório. Em vez disso, o "Code Red II" mantém a parte da rede do endereço IP e escolhe uma parte aleatória do host do endereço IP para se propagar. Isso permite que o worm se espalhe mais rapidamente na mesma rede.

O "Código Vermelho II" usa estas redes e máscaras:

```
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)
```

Os endereços IP de destino excluídos são 127.X.X.X e 224.X.X.X, e nenhum octeto tem permissão para ser 0 ou 255. Além disso, o host não tenta se infectar novamente.

Para obter mais informações, consulte o Código Vermelho (II) .

Às vezes, não é possível executar o netflow para detectar uma tentativa de infestação "Code Red". Isso pode ocorrer porque você executa uma versão de código que não suporta o netflow ou porque o roteador tem memória insuficiente ou excessivamente fragmentada para ativar o netflow. A Cisco recomenda que você não ative o netflow quando houver várias interfaces de entrada e apenas uma interface de saída no roteador, pois a contabilidade do netflow é executada no caminho de entrada. Nesse caso, é melhor habilitar a contabilização de IP na interface de saída isolada.

Observação: o comando ip accounting desativa o DCEF. Não habilite a contabilidade IP em nenhuma plataforma onde você queira usar a comutação 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
```

Na saída do comando show ip accounting, procure os endereços de origem que tentam enviar pacotes para vários endereços de destino. Se o host infectado estiver na fase de varredura, ele tentará estabelecer conexões HTTP com outros roteadores. Assim, você verá tentativas de acessar vários endereços IP. A maioria dessas tentativas de conexão normalmente falham. Portanto, você vê apenas um pequeno número de pacotes transferidos, cada um com uma pequena contagem de bytes. Neste exemplo, é provável que 20.1.145.49 e 20.1.104.194 estejam infectados.

Quando você executa o MLS (Multi-Layer Switching) no Catalyst 5000 Series e no Catalyst 6000 Series, você deve tomar diferentes etapas para ativar o relatório de Netflow e rastrear a infestação. Em um switch Cat6000 equipado com Supervisor 1 Multilayer Switch Feature Card

(MSFC1) ou SUP I/MSFC2, o MLS baseado em netflow é ativado por padrão, mas o modo de fluxo é somente de destino. Portanto, o endereço IP origem não está em cache. Você pode ativar o modo de "fluxo completo" para rastrear hosts infectados com a ajuda do comando **set mls flow full** no supervisor.

Para o modo Híbrido, use o 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.
```

Para o modo IOS nativo, use o comando **mls flow ip full**:

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

Quando você ativa o modo de "fluxo completo", um aviso é exibido para indicar um aumento significativo nas entradas de MLS. O impacto das entradas MLS aumentadas é justificável por um curto período se sua rede já estiver infestada com o worm "Code Red". O worm faz com que suas entradas MLS sejam excessivas e aumentem.

Para exibir as informações coletadas, use estes comandos:

Para o modo Híbrido, use o 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.
```

Para o modo Native IOS, use o comando **mls flow ip full**:

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

Quando você ativa o modo de "fluxo completo", um aviso é exibido para indicar um aumento significativo nas entradas de MLS. O impacto das entradas MLS aumentadas é justificável por um curto período se sua rede já estiver infestada com o worm "Code Red". O worm faz com que suas entradas MLS sejam excessivas e aumentem.

Para exibir as informações coletadas, use estes comandos:

Para o modo Híbrido, use o 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
--------------- --------------- ----- ------ ------ ----------------- ---- ----
---- --------- --------- ---------- ----------- -------- --------
```

Observação: todos esses campos são preenchidos quando estão no modo de "fluxo completo".

Para o modo IOS nativo, use o comando **show mls ip**:

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

Ao determinar o endereço IP origem e a porta destino envolvidos no ataque, você pode redefinir o MLS para o modo "apenas destino".

Para o modo Híbrido, use o comando **set mls flow destination**:

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

Para o modo IOS nativo, use o comando **mls flow ip destination**:

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

A combinação Supervisor (SUP) II/MSFC2 é protegida contra ataques porque a comutação CEF é executada no hardware e as estatísticas de netflow são mantidas. Assim, mesmo durante um ataque "Code Red", se você habilitar o modo de fluxo completo, o roteador não será trocado por causa do mecanismo de switching mais rápido. Os comandos para ativar o modo de fluxo completo e exibir as estatísticas são os mesmos no SUP I/MFSC1 e no SUP II/MSFC2.

Técnicas de prevenção

Use as técnicas listadas nesta seção para minimizar o impacto do worm "Code Red" no roteador.

Bloquear tráfego para a porta 80

Se isso for viável em sua rede, a maneira mais fácil de evitar o ataque do "Código Vermelho" é bloquear todo o tráfego para a porta 80, que é a porta bem conhecida para WWW. Crie uma lista de acesso para negar pacotes IP destinados à porta 80 e aplique-a na entrada da interface que enfrenta a origem da infecção.

Reduza o uso da memória de entrada ARP

A entrada ARP usa grandes quantidades de memória quando uma rota estática aponta para uma interface de broadcast, como esta:

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

Cada pacote para a rota padrão é enviado para a VLAN3. No entanto, não há endereço IP do próximo salto especificado e, portanto, o roteador envia uma solicitação ARP para o endereço IP de destino. O roteador do próximo salto para esse destino responde com seu próprio endereço MAC, a menos que o Proxy ARP esteja desabilitado. A resposta do roteador cria uma entrada adicional na tabela ARP onde o endereço IP destino do pacote é mapeado para o endereço MAC do próximo salto. O worm "Code Red" envia pacotes para endereços IP aleatórios, o que adiciona uma nova entrada ARP para cada endereço de destino aleatório. Cada nova entrada ARP consome cada vez mais memória no processo de entrada ARP.

Não crie uma rota padrão estática para uma interface, especialmente se a interface for broadcast (Ethernet/Fast Ethernet/GE/SMDS) ou multiponto (Frame Relay/ATM). Qualquer rota padrão estática deve apontar para o endereço IP do roteador do próximo salto. Depois de alterar a rota padrão para apontar para o endereço IP do próximo salto, use o **comando clear arp-cache** para limpar todas as entradas ARP. Esse comando corrige o problema de utilização da memória.

Usar o switching do Cisco Express Forwarding (CEF)

Para reduzir a utilização da CPU em um roteador IOS, mude de switching Fast/Optimum/Netflow para switching CEF. Há algumas advertências para ativar o CEF. A próxima seção discute a diferença entre CEF e fast switching e explica as implicações quando você habilita CEF.

Cisco Express Forwarding versus Fast Switching

Habilite o CEF para aliviar o aumento da carga de tráfego causado pelo worm "Code Red". Os Cisco IOS® Software Releases 11.1( )CC, 12.0 e posteriores suportam CEF nas plataformas Cisco 7200/7500/GSR. O suporte para CEF em outras plataformas está disponível no Cisco IOS Software Release 12.0 ou posterior. Você pode investigar mais com a ferramenta Software Advisor.

Às vezes, não é possível habilitar o CEF em todos os roteadores devido a um destes motivos:

- Memória insuficiente
- Arquiteturas de plataforma não suportadas
- Encapsulamentos de interface não suportados

Comportamento e implicações do Fast Switching

Aqui estão as implicações quando você usa a switching rápida:

- Cache acionado por tráfego—O cache fica vazio até que o roteador comute os pacotes e preencha o cache.
- O primeiro pacote é comutado por processo—O primeiro pacote é comutado por processo, porque o cache está inicialmente vazio.
- Cache granular—O cache é construído com uma granularidade da parte de entrada da Base de Informações de Roteamento (RIB - Routing Information Base) mais específica de uma rede principal. Se o RIB tiver /24s para a rede principal 131.108.0.0, o cache será construído com /24s para esta rede principal.
- O cache /32 é usado— o cache /32 é usado para balancear a carga para cada destino. Quando o cache equilibra a carga, o cache é construído com /32s para a rede principal.**Observação:** esses dois últimos problemas podem causar um enorme cache que consumiria toda a memória.
- Cache nos principais limites da rede—Com a rota padrão, o cache é executado nos principais limites da rede.
- O Cache Ager—O cache ager executa a cada minuto e verifica 1/20 (5%) do cache para entradas não utilizadas em condições normais de memória e 1/4 (25%) do cache em uma condição de memória baixa (200 k).

Para alterar os valores acima, use o **comando ip cache-ager-interval X Y Z**, onde:

- X é <0-2147483> número de segundos entre execuções de ager. Padrão = 60 segundos.
- Y é <2-50> 1/(Y+1) do cache para envelhecer por execução (memória baixa). Padrão = 4.
- Z é <3-100> 1/(Z+1) do cache para envelhecer por execução (normal). Padrão = 20.

Aqui está um exemplo de configuração que usa o **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
```

Com base na configuração do seu cache ager, alguma porcentagem das entradas de cache envelhece da sua tabela de cache rápido. Quando as entradas envelhecem rapidamente, uma porcentagem maior da tabela de cache rápido envelhece e a tabela de cache se torna menor. Como resultado, o consumo de memória no roteador é reduzido. Uma desvantagem é que o tráfego continua a fluir para as entradas que foram retiradas da tabela de cache. Os pacotes iniciais são comutados por processo, o que causa um pequeno pico no consumo da CPU na **entrada IP** até que uma nova entrada de cache seja criada para o fluxo.

Nas versões 10.3(8), 11.0(3) e posteriores do software Cisco IOS, o agente de cache IP é tratado de forma diferente, como explicado aqui:

- Os comandos **ip cache-ager-interval** e **ip cache-invalid-delay** estarão disponíveis somente se o comando **service internal** estiver definido na configuração.
- Se o período entre as execuções de invalidação do ager estiver definido como 0, o processo do ager será totalmente desabilitado.
- O tempo é expresso em segundos.

Observação: quando você executa esses comandos, a utilização da CPU do roteador aumenta. Use esses comandos somente quando absolutamente necessário.

```
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
```

Vantagens do CEF

- A tabela FIB (Forwarding Information Base) é criada com base na tabela de roteamento. Portanto, as informações de encaminhamento existem antes do primeiro pacote ser encaminhado. O FIB também contém /32 entradas para hosts de LAN conectados diretamente.
- A tabela ADJ (Adjacency, adjacência) contém as informações de regravação da camada 2 para os próximos saltos e hosts conectados diretamente (uma entrada ARP cria uma adjacência CEF).
- Não há conceito de envelhecimento de cache com CEF para aumentar a utilização de CPU. Uma entrada FIB será excluída se uma entrada da tabela de roteamento for excluída.

Cuidado: novamente, uma rota padrão que aponta para uma interface de broadcast ou multiponto significa que o roteador envia solicitações ARP para cada novo destino. As solicitações ARP do roteador podem criar uma enorme tabela de adjacência até que o roteador fique sem memória. Se o CEF não alocar memória, o CEF/DCEF se desabilita. Você precisará habilitar manualmente CEF/DCEF novamente.

Saída de exemplo: CEF

Aqui estão alguns exemplos de saída do comando show ip cef summary, que mostra o uso da memória. Esta saída é um instantâneo de um servidor de rota Cisco 7200 com o Cisco IOS Software Release 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
```

Pontos a serem considerados

Quando o número de fluxos é grande, o CEF geralmente consome menos memória do que a comutação rápida. Se a memória já for consumida por um cache de switching rápida, você deve limpar o cache ARP (através do comando **clear ip arp**) antes de habilitar o CEF.

Observação: ao limpar o cache, um pico é causado na utilização da CPU do roteador.

Perguntas frequentes sobre o "Código vermelho" e suas respostas

P. Eu uso NAT e experimento 100% de utilização da CPU na entrada IP. Quando executo show proc cpu, minha utilização da CPU é alta no nível de interrupção - 100/99 ou 99/98. Isso pode ser relacionado ao "Código Vermelho"?

A. Recentemente, foi corrigido um bug da Cisco NAT (CSCdu63623 (somente clientes registrados)) que envolve escalabilidade. Quando há dezenas de milhares de fluxos de NAT (com base no tipo de plataforma), o bug causa 100% de utilização da CPU no nível de processo ou interrupção.

Para determinar se esse bug é o motivo, execute o comando **show align** e verifique se o roteador enfrenta erros de alinhamento. Se você vir erros de alinhamento ou acessos artificiais à memória, execute o comando **show align** algumas vezes e veja se os erros estão aumentando. Se o número de erros está aumentando, os erros de alinhamento podem ser a causa da alta utilização da CPU no nível de interrupção, e não o bug da Cisco CSCdu63623 (somente clientes registrados) . Para obter mais informações, consulte Solução de problemas de acessos artificiais e erros de alinhamento.

O comando **show ip nat translation** exibe o número de conversões ativas. O ponto de fusão de um processador da classe NPE-300 é de aproximadamente 20.000 a 40.000 traduções. Esse número varia de acordo com a plataforma.

Esse problema de colapso foi observado anteriormente por alguns clientes, mas depois do "Código Vermelho", mais clientes passaram por esse problema. A única solução é executar o NAT (em vez de PAT), para que haja menos traduções ativas. Se você tiver um 7200, use um NSE-1 e reduza os valores de tempo limite de NAT.

P. Executo o IRB e encontro alta utilização da CPU no processo de entrada do HyBridge. Por que isso acontece? Tem alguma relação com "Código Vermelho"?

A. O processo HyBridge Input lida com todos os pacotes que não podem ser comutados rapidamente pelo processo IRB. A incapacidade do processo IRB para comutar rapidamente um pacote pode ser porque:

- O pacote é um pacote de broadcast.
- O pacote é um pacote multicast.
- O destino é desconhecido e o ARP precisa ser acionado.
- Há BPDUs de spanning tree.

A entrada HyBridge encontra problemas se houver milhares de interfaces ponto-a-ponto no mesmo grupo de bridge. A entrada da HyBridge também encontra problemas (mas em menor escala) se houver milhares de VSs na mesma interface multiponto.

Quais são os motivos possíveis para problemas com IRB? Suponha que um dispositivo infectado com o código vermelho verifique os endereços IP.

- O roteador precisa enviar uma solicitação ARP para cada endereço IP de destino. Uma inundação de solicitações ARP resulta em cada VC do grupo de bridge para cada endereço que é analisado. O processo ARP normal não causa um problema na CPU. No entanto, se houver uma entrada ARP sem uma entrada de bridge, o roteador inunda pacotes destinados a endereços para os quais já existem entradas ARP. Isso poderá causar uma alta utilização de CPU, pois o tráfego é comutado pelo processo. Para evitar o problema, aumente o tempo

de envelhecimento da ponte (padrão de 300 segundos ou 5 minutos) para corresponder ou exceder o tempo limite do ARP (padrão de 4 horas) para que os dois temporizadores sejam sincronizados.
- O endereço que o host final tenta infectar é um endereço de broadcast. O roteador faz o equivalente a uma difusão de sub-rede que precisa ser replicada pelo processo HyBridge Input (Entrada de HyBridge). Isso não acontece se o comando **no ip directed-broadcast** estiver configurado. No Cisco IOS Software Release 12.0, o comando **ip directed-broadcast** é desativado por padrão, o que faz com que todos os broadcasts direcionados por IP sejam descartados.
- Aqui está uma nota complementar, não relacionada ao "Code Red" e relacionada às arquiteturas IRB:Os pacotes multicast e broadcast da camada 2 precisam ser replicados. Portanto, um problema com servidores IPX executados em um segmento de broadcast pode desativar o link. Você pode usar políticas de assinante para evitar o problema. Para obter mais informações, consulte Suporte a Bridge x Digital Subscriber Line (xDSL). Você também deve considerar as listas de acesso de bridge, que limitam o tipo de tráfego permitido para passar pelo roteador.
- Para aliviar esse problema de IRB, você pode usar vários grupos de bridge e garantir que haja um mapeamento um para um para BVIs, subinterfaces e VCs.
- O RBE é superior ao IRB porque evita a pilha de Bridging. Você pode migrar para o RBE do IRB. Esses bugs da Cisco inspiram essa migração:CSCdr11146 (apenas clientes registrados)CSCdp18572 (apenas clientes registrados)CSCds40806 (apenas clientes registrados)

P. A utilização da CPU é alta no nível de interrupção e recebo liberações se eu tentar mostrar registro. A taxa de tráfego também está um pouco superior ao normal. Qual é a razão para isso?

A. Aqui está um exemplo da saída do 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
```

Verifique se você fez login no console. Em caso afirmativo, verifique se há solicitações HTTP de tráfego. Em seguida, verifique se há alguma lista de acesso com palavras-chave de log ou depurações que observam fluxos IP específicos. Se as descargas estiverem em alta, pode ser porque o console, geralmente um dispositivo de 9600 baud, não consegue lidar com a quantidade de informações recebidas. Neste cenário, o roteador desativa interrupções e não faz nada além de processar mensagens do console. A solução é desabilitar o registro do console ou remover qualquer tipo de registro executado.

P. Posso ver várias tentativas de conexão HTTP em meu roteador IOS que executa um ip http-server. Isso é devido ao exame de worm "Código vermelho"?

R. "Código Vermelho" pode ser o motivo aqui. A Cisco recomenda que você desative o comando **ip http server** no roteador IOS para que ele não precise lidar com numerosas tentativas de conexão de hosts infectados.

Soluções

Há várias soluções alternativas que são discutidas na seção Consultoria que discute o worm "Código vermelho". Consulte as recomendações para as soluções alternativas.

Outro método para bloquear o worm "Code Red" nos pontos de entrada da rede usa o NBAR (Network-Based Application Recognition, reconhecimento de aplicativos baseados em rede) e as ACLs (Access Control Lists, listas de controle de acesso) no software IOS nos roteadores Cisco. Use este método em conjunto com os patches recomendados para servidores IIS da Microsoft. Para obter mais informações sobre esse método, consulte Utilização de NBAR e ACLs para Bloquear o Worm "Código Vermelho" em Pontos de Entrada de Rede.

Informações Relacionadas

- Troubleshooting Problemas de Memória
- Troubleshooting de Vazamentos de Buffer
- Troubleshooting de Alta Utilização de CPU em Cisco Routers
- Troubleshooting de Travamentos de Roteador
- Notas técnicas de solução de problemas - Roteadores
- Troubleshooting do Roteador
- Suporte Técnico e Documentação - Cisco Systems