Réponse à un cas d'erreur mallocfail ou d'utilisation élevée du processeur résultant du ver « Code Red »

Contenu

Introduction

Ce document décrit le ver « Code Red » et les problèmes que ce ver peut causer dans un

environnement de routage Cisco. Ce document décrit également les techniques de prévention de l'infestation du ver et fournit des liens vers des avis connexes qui décrivent des solutions aux problèmes liés aux vers.

Le ver « Code Red » exploite une vulnérabilité dans le service d'index de Microsoft Internet Information Server (IIS) version 5.0. Lorsque le ver « Code Red » infecte un hôte, il le fait sonder et infecter une série aléatoire d'adresses IP, ce qui entraîne une forte augmentation du trafic réseau. Ceci est particulièrement problématique s'il existe des liaisons redondantes dans le réseau et/ou Cisco Express Forwarding (CEF) n'est pas utilisé pour commuter des paquets.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Comment le ver « Code Red » infecte d'autres systèmes

Le ver « Code Red » tente de se connecter à des adresses IP générées aléatoirement. Chaque serveur IIS infecté peut tenter d'infecter le même ensemble de périphériques. Vous pouvez suivre l'adresse IP source et le port TCP du ver, car il n'est pas usurpé. Le transfert de chemin inverse de monodiffusion (URPF) ne peut pas supprimer une attaque de ver, car l'adresse source est légale.

Conseils relatifs au ver « Code Red »

Ces conseils décrivent le ver « Code Red » et expliquent comment corriger les logiciels affectés par le ver :

- Avis de sécurité Cisco : Vers « Code Red » - Impact sur le client
- Débordement de la mémoire tampon d'extension ISAPI du serveur d'index IIS distant
- Vers .ida « Code Red »
- CERT ? Avis CA-2001-19 « Code Red » Exploiter le débordement de tampon dans la DLL du service d'indexation IIS

Symptômes

Voici quelques symptômes qui indiquent qu'un routeur Cisco est affecté par le ver « Code Red » :

- Grand nombre de flux dans les tables NAT ou PAT (si vous utilisez NAT ou PAT).
- Nombre important de requêtes ARP ou de tempêtes ARP dans le réseau (causées par l'analyse d'adresse IP).
- Utilisation excessive de mémoire par les processus IP Input, ARP Input, IP Cache Ager et CEF.
- Utilisation élevée du CPU dans ARP, IP Input, CEF et IPC.
- Utilisation élevée du CPU au niveau d'interruption à des débits de trafic faibles, ou utilisation élevée du CPU au niveau du processus dans l'entrée IP, si vous utilisez NAT.

Une condition de mémoire faible ou une utilisation élevée et soutenue du CPU (100 %) au niveau d'interruption peut entraîner le rechargement d'un routeur Cisco IOS®. Le rechargement est provoqué par un processus qui se comporte mal en raison des conditions de contrainte.

Si vous ne soupçonnez pas que les périphériques de votre site sont infectés par ou sont la cible du ver « Code Red », reportez-vous à la section Informations connexes pour obtenir des URL supplémentaires sur la façon de résoudre les problèmes que vous rencontrez.

Identifier le périphérique infecté

Utilisez la commutation de flux pour identifier l'adresse IP source du périphérique affecté. Configurez ip route-cache flow sur toutes les interfaces pour enregistrer tous les flux commutés par le routeur.

Après quelques minutes, exécutez la commande show ip cache flow pour afficher les entrées enregistrées. Au cours de la phase initiale de l'infection par le ver « Code Red », le ver essaie de se reproduire. La réplication se produit lorsque le ver envoie des requêtes HT à des adresses IP aléatoires. Par conséquent, vous devez rechercher des entrées de flux de cache avec le port de destination 80 (HT., 0050 en hexadécimal).

La commande **show ip cache flow | include 0050** affiche toutes les entrées de cache avec un port TCP 80 (0050 en hexadécimal) :

```
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
```

Si vous trouvez un nombre anormalement élevé d'entrées avec la même adresse IP source, l'adresse IP de destination aléatoire [1], DstP = 0050 (HTTP) et Pr = 06 (TCP), vous avez

probablement localisé un périphérique infecté. Dans cet exemple de sortie, l'adresse IP source est 193.23.45.35 et provient de VLAN1.

[1] Une autre version du ver « Code Red », appelé « Code Red II », ne choisit pas une adresse IP de destination totalement aléatoire. Au lieu de cela, « Code Red II » conserve la partie réseau de l'adresse IP et choisit une partie hôte aléatoire de l'adresse IP afin de se propager. Cela permet au ver de se propager plus rapidement dans le même réseau.

« Code Red II » utilise ces réseaux et masques :

```
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)
```

Les adresses IP cibles exclues sont 127.X.X.X et 224.X.X.X et aucun octet ne peut être 0 ou 255. En outre, l'hôte ne tente pas de se réinfecter.

Pour plus d'informations, consultez Code Red (II) .

Parfois, vous ne pouvez pas exécuter netflow pour détecter une tentative d'infestation « Code Red ». Cela peut être dû au fait que vous exécutez une version de code qui ne prend pas en charge netflow, ou parce que le routeur a une mémoire insuffisante ou excessivement fragmentée pour activer netflow. Cisco recommande de ne pas activer netflow lorsqu'il existe plusieurs interfaces d'entrée et une seule interface de sortie sur le routeur, car la comptabilité netflow est exécutée sur le chemin d'entrée. Dans ce cas, il est préférable d'activer la comptabilité IP sur l'interface de sortie unique.

Remarque : La commande ip accounting désactive DCEF. N'activez pas la comptabilité IP sur une plate-forme sur laquelle vous souhaitez utiliser la commutation 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
```

Dans le résultat de la commande show ip accounting, recherchez les adresses source qui tentent d'envoyer des paquets à plusieurs adresses de destination. Si l'hôte infecté est en phase d'analyse, il tente d'établir des connexions HTTP avec d'autres routeurs. Ainsi, vous verrez des

tentatives d'accès à plusieurs adresses IP. La plupart de ces tentatives de connexion échouent normalement. Par conséquent, vous ne voyez qu'un petit nombre de paquets transférés, chacun avec un petit nombre d'octets. Dans cet exemple, il est probable que 20.1.145.49 et 20.1.104.194 soient infectés.

Lorsque vous exécutez la commutation multicouche (MLS) sur les gammes Catalyst 5000 et Catalyst 6000, vous devez prendre différentes mesures pour activer la comptabilité netflow et suivre l'infestation. Dans un commutateur Cat6000 équipé d'une carte MSFC1 (Supervisor 1 Multilayer Switch Feature Card) ou d'une carte SUP I/MSFC2, la fonction MLS basée sur netflow est activée par défaut, mais le mode flux est uniquement de destination. Par conséquent, l'adresse IP source n'est pas mise en cache. Vous pouvez activer le mode « flux complet » pour suivre les hôtes infectés à l'aide de la commande **set mls flow full** sur le superviseur.

Pour le mode hybride, utilisez la commande **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.
```

Pour le mode IOS natif, utilisez la commande **mls flow ip full** :

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

Lorsque vous activez le mode « flux complet », un avertissement s'affiche pour indiquer une augmentation spectaculaire des entrées MLS. L'impact de l'augmentation des entrées MLS est justifiable pour une courte durée si votre réseau est déjà infesté par le ver « Code Red ». Le ver provoque un excès de vos entrées MLS et une augmentation.

Pour afficher les informations collectées, utilisez les commandes suivantes :

Pour le mode hybride, utilisez la commande **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.
```

Pour le mode IOS natif, utilisez la commande **mls flow ip full** :

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

Lorsque vous activez le mode « flux complet », un avertissement s'affiche pour indiquer une augmentation spectaculaire des entrées MLS. L'impact de l'augmentation des entrées MLS est justifiable pour une courte durée si votre réseau est déjà infesté par le ver « Code Red ». Le ver provoque un excès de vos entrées MLS et une augmentation.

Pour afficher les informations collectées, utilisez les commandes suivantes :

Pour le mode hybride, utilisez la commande **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
-------------- -------------- ----- ------ ------ ----------------- ---- ----
---- --------- --------- ---------- ----------- -------- --------
```

Note : Tous ces champs sont remplis lorsqu'ils sont en mode « plein flux ».

Pour le mode IOS natif, utilisez la commande **show mls ip** :

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

Lorsque vous déterminez l'adresse IP source et le port de destination impliqués dans l'attaque, vous pouvez rétablir le mode MLS en mode « destination uniquement ».

Pour le mode hybride, utilisez la commande **set mls flow destination** :

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

Pour le mode IOS natif, utilisez la commande **mls flow ip destination** :

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

La combinaison Supervisor (SUP) II/MSFC2 est protégée contre les attaques car la commutation CEF est effectuée dans le matériel et les statistiques de flux réseau sont mises à jour. Ainsi, même lors d'une attaque « Code Red », si vous activez le mode plein débit, le routeur n'est pas submergé, en raison du mécanisme de commutation plus rapide. Les commandes permettant d'activer le mode flux total et d'afficher les statistiques sont les mêmes sur SUP I/MFSC1 et SUP II/MSFC2.

Techniques de prévention

Utilisez les techniques répertoriées dans cette section pour minimiser l'impact du ver « Code Red » sur le routeur.

Bloquer le trafic vers le port 80

Si cela est possible sur votre réseau, le moyen le plus simple d'empêcher l'attaque « Code Red » est de bloquer tout le trafic vers le port 80, qui est le port le plus connu pour WWW. Créez une liste d'accès pour refuser les paquets IP destinés au port 80 et appliquez-la en entrée sur l'interface qui fait face à la source d'infection.

Réduction de l'utilisation de la mémoire ARP en entrée

L'entrée ARP consomme une quantité énorme de mémoire lorsqu'une route statique pointe vers une interface de diffusion, comme ceci :

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

Chaque paquet pour la route par défaut est envoyé au VLAN3. Cependant, aucune adresse IP de tronçon suivant n'est spécifiée. Par conséquent, le routeur envoie une requête ARP pour l'adresse IP de destination. Le routeur de tronçon suivant de cette destination répond avec sa propre adresse MAC, sauf si Proxy ARP est désactivé. La réponse du routeur crée une entrée supplémentaire dans la table ARP où l'adresse IP de destination du paquet est mappée à l'adresse MAC de tronçon suivant. Le ver « Code Red » envoie des paquets aux adresses IP aléatoires, ce qui ajoute une nouvelle entrée ARP pour chaque adresse de destination aléatoire. Chaque nouvelle entrée ARP consomme de plus en plus de mémoire dans le processus d'entrée ARP.

Ne créez pas de route statique par défaut vers une interface, en particulier si l'interface est de diffusion (Ethernet/Fast Ethernet/GE/SMDS) ou multipoint (Frame Relay/ATM). Toute route statique par défaut doit pointer vers l'adresse IP du routeur du tronçon suivant. Après avoir modifié la route par défaut pour pointer vers l'adresse IP du tronçon suivant, utilisez la commande **clear arp-cache** pour effacer toutes les entrées ARP. Cette commande corrige le problème d'utilisation de la mémoire.

Utiliser la commutation CEF (Cisco Express Forwarding)

Afin de réduire l'utilisation du CPU sur un routeur IOS, passez de la commutation Fast/Optimum/Netflow à la commutation CEF. Il y a quelques mises en garde pour activer CEF. La section suivante traite de la différence entre CEF et la commutation rapide et explique les implications lorsque vous activez CEF.

Cisco Express Forwarding et Fast Switching

Activez CEF pour alléger la charge de trafic accrue causée par le ver « Code Red ». Le logiciel Cisco IOS® versions 11.1( )CC, 12.0 et ultérieures prennent en charge CEF sur les plates-formes Cisco 7200/7500/GSR. La prise en charge de CEF sur d'autres plates-formes est disponible dans le logiciel Cisco IOS Version 12.0 ou ultérieure. Vous pouvez approfondir vos recherches avec l'outil Software Advisor.

Parfois, vous ne pouvez pas activer CEF sur tous les routeurs pour l'une des raisons suivantes :

- Mémoire insuffisante
- Architectures de plate-forme non prises en charge
- Encapsulations d'interface non prises en charge

Comportement et implications de la commutation rapide

Voici les implications de la commutation rapide :

- Cache piloté par le trafic : le cache est vide jusqu'à ce que le routeur commute les paquets et renseigne le cache.
- Premier paquet à commutation de processus : le premier paquet est à commutation de processus, car le cache est initialement vide.
- Cache granulaire : le cache est construit à une granularité de la partie d'entrée RIB (Routing Information Base) la plus spécifique d'un réseau principal. Si RIB a /24s pour le réseau principal 131.108.0.0, le cache est construit avec /24s pour ce réseau principal.

- Le cache /32 est utilisé : le cache /32 sert à équilibrer la charge pour chaque destination. Lorsque le cache équilibre la charge, le cache est construit avec /32 pour ce réseau principal.**Remarque :** Ces deux derniers problèmes peuvent potentiellement entraîner un énorme cache qui consommerait toute la mémoire.
- Mise en cache aux frontières du réseau principal : avec la route par défaut, la mise en cache est effectuée aux frontières du réseau principal.
- L'agent de cache : le gestionnaire de cache s'exécute toutes les minutes et vérifie le 1/20e (5 %) du cache pour les entrées inutilisées dans des conditions de mémoire normales, et le 1/4e (25 %) du cache dans une condition de mémoire faible (200 Ko).

Afin de modifier les valeurs ci-dessus, utilisez la commande **ip cache-ager-interval X Y Z**, où :

- X représente <0-2147483> nombre de secondes entre les exécutions de la radiomessagerie. Valeur par défaut = 60 secondes.
- Y représente <2-50> 1/(Y+1) de mémoire cache par série (mémoire insuffisante). Valeur par défaut = 4.
- Z représente <3-100> 1/(Z+1) de mémoire cache par période (normale). Par défaut = 20.

Voici un exemple de configuration qui utilise **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
```

En fonction du paramètre de votre ager de cache, un certain pourcentage des entrées de votre cache expire dans votre table de cache rapide. Lorsque les entrées vieillissent rapidement, un plus grand pourcentage de la table de cache rapide vieillit et la table de cache devient plus petite. En conséquence, la consommation de mémoire sur le routeur diminue. Un inconvénient est que le trafic continue à circuler pour les entrées qui ont été vieillies de la table de cache. Les paquets initiaux sont commutés par processus, ce qui entraîne une augmentation rapide de la consommation de CPU dans l'**entrée IP** jusqu'à ce qu'une nouvelle entrée de cache soit créée pour le flux.

Àpartir des versions 10.3(8), 11.0(3) et ultérieures du logiciel Cisco IOS, le gestionnaire de cache

IP est géré différemment, comme expliqué ici :

- Les commandes **ip cache-ager-interval** et **ip cache-invalider-delay** ne sont disponibles que si la commande **service internal** est définie dans la configuration.
- Si la période entre les exécutions d'invalidation de l'amplificateur est définie sur 0, le processus de l'amplificateur est entièrement désactivé.
- Le temps est exprimé en secondes.

Remarque : lorsque vous exécutez ces commandes, l'utilisation du processeur du routeur augmente. Utilisez ces commandes uniquement lorsque cela est absolument nécessaire.

```
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
```

Avantages du CEF

- La table FIB (Forwarding Information Base) est construite en fonction de la table de routage. Par conséquent, des informations de transmission existent avant le transfert du premier paquet. La FIB contient également des entrées /32 pour les hôtes LAN connectés directement.
- La table de contiguïté (ADJ) contient les informations de réécriture de couche 2 pour les sauts suivants et les hôtes directement connectés (une entrée ARP crée une contiguïté CEF).
- Il n'existe aucun concept de mise en cache avec CEF pour augmenter l'utilisation du CPU. Une entrée FIB est supprimée si une entrée de table de routage est supprimée.

Attention : Une fois de plus, une route par défaut qui pointe vers une interface de diffusion ou multipoint signifie que le routeur envoie des requêtes ARP pour chaque nouvelle destination. Les requêtes ARP du routeur peuvent créer une table de contiguïté énorme jusqu'à ce que le routeur manque de mémoire. Si CEF ne parvient pas à allouer de la mémoire CEF/DCEF se désactive. Vous devrez réactiver CEF/DCEF manuellement.

Exemple de sortie : CEF

Voici un exemple de sortie de la commande show ip cef summary, qui montre l'utilisation de la mémoire. Ce résultat est un instantané d'un serveur de routage Cisco 7200 avec le logiciel Cisco IOS Version 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
```

Éléments à prendre en compte

Lorsque le nombre de flux est important, CEF consomme généralement moins de mémoire que la commutation rapide. Si la mémoire est déjà utilisée par un cache de commutation rapide, vous devez effacer le cache ARP (via la commande **clear ip arp**) avant d'activer CEF.

Remarque : lorsque vous effacez le cache, une pointe est provoquée dans l'utilisation du processeur du routeur.

Foire aux questions « Code Red » et leurs réponses

Q. J'utilise la NAT et j'utilise 100 % du CPU en entrée IP. Lorsque j'exécute show proc cpu, mon utilisation du CPU est élevée en niveau d'interruption - 100/99 ou 99/98. Est-ce que cela peut être lié à « Code Red » ?

A. Un bogue NAT de Cisco (CSCdu63623 (clients enregistrés uniquement) a été récemment corrigé. Lorsqu'il y a des dizaines de milliers de flux NAT (basés sur le type de plate-forme), le bogue entraîne une utilisation de 100 % du CPU au niveau du processus ou de l'interruption.

Afin de déterminer si ce bogue est la raison, émettez la commande **show align**, et vérifiez si le routeur est confronté à des erreurs d'alignement. Si des erreurs d'alignement ou des accès à la mémoire erronés s'affichent, émettez la commande **show align** à quelques reprises et vérifiez si les erreurs sont en augmentation. Si le nombre d'erreurs augmente, les erreurs d'alignement peuvent être la cause d'une utilisation élevée du CPU au niveau d'interruption, et non le bogue Cisco CSCdu63623 (clients enregistrés uniquement). Pour plus d'informations, référez-vous à Dépannage des accès indésirables et des erreurs d'alignement.

La commande **show ip nat translation** affiche le nombre de traductions actives. Le point de fusion d'un processeur de classe NPE-300 est d'environ 20 000 à 40 000 traductions. Ce nombre varie selon la plate-forme.

Ce problème d'effondrement a déjà été observé par quelques clients, mais après « Code Red », plus de clients ont connu ce problème. La seule solution consiste à exécuter NAT (au lieu de PAT), de sorte qu'il y ait moins de traductions actives. Si vous avez un 7200, utilisez un NSE-1 et diminuez les valeurs de délai d'attente NAT.

Q. J'exécute IRB et je rencontre une utilisation élevée du CPU dans le processus d'entrée HyBridge. Que se passe-t-il ? Est-ce lié à « Code Red » ?

A. Le processus d'entrée HyBridge gère tous les paquets qui ne peuvent pas être commutés rapidement par le processus IRB. L'incapacité du processus IRB à commuter rapidement un paquet peut être due à :

- Le paquet est un paquet de diffusion.
- Le paquet est un paquet de multidiffusion.
- La destination est inconnue et le protocole ARP doit être déclenché.
- Il existe des BPDU Spanning Tree.

HyBridge Input rencontre des problèmes s'il y a des milliers d'interfaces point à point dans le

même groupe de ponts. HyBridge Input rencontre également des problèmes (mais dans une moindre mesure) s'il y a des milliers de VS dans la même interface multipoint.

Quelles sont les raisons possibles des problèmes liés à la CISR? Supposons qu'un périphérique infecté par le code rouge analyse les adresses IP.

- Le routeur doit envoyer une requête ARP pour chaque adresse IP de destination. Un flot de requêtes ARP résulte sur chaque circuit virtuel du groupe de pontage pour chaque adresse analysée. Le processus ARP normal ne cause pas de problème de CPU. Cependant, s'il existe une entrée ARP sans entrée de pont, le routeur diffuse les paquets destinés aux adresses pour lesquelles des entrées ARP existent déjà. Cela peut entraîner une utilisation élevée du CPU, car le trafic est commuté par processus. Pour éviter le problème, augmentez le délai de vieillissement du pont (300 secondes ou 5 minutes par défaut) pour correspondre ou dépasser le délai ARP (4 heures par défaut) de sorte que les deux temporisateurs soient synchronisés.
- L'adresse que l'hôte final tente d'infecter est une adresse de diffusion. Le routeur effectue l'équivalent d'une diffusion de sous-réseau qui doit être répliquée par le processus d'entrée HyBridge. Cela ne se produit pas si la commande **no ip directed-broadcast** est configurée. À partir du logiciel Cisco IOS Version 12.0, la commande **ip directed-broadcast** est désactivée par défaut, ce qui entraîne l'abandon de toutes les diffusions dirigées par IP.
- Voici une note secondaire, sans rapport avec « Code Red », et liée aux architectures IRB :Les paquets de multidiffusion et de diffusion de couche 2 doivent être répliqués. Par conséquent, un problème avec les serveurs IPX qui s'exécutent sur un segment de diffusion peut mettre la liaison hors service. Vous pouvez utiliser des stratégies d'abonné pour éviter le problème. Pour plus d'informations, référez-vous à la prise en charge de x Digital Subscriber Line (xDSL) Bridge. Vous devez également tenir compte des listes d'accès de pont, qui limitent le type de trafic autorisé à traverser le routeur.
- Afin d'atténuer ce problème IRB, vous pouvez utiliser plusieurs groupes de ponts et vous assurer qu'il existe un mappage un-à-un pour les BVI, les sous-interfaces et les circuits virtuels.
- RBE est supérieur à IRB car il évite complètement la pile de pontage. Vous pouvez migrer vers RBE depuis IRB. Ces bogues Cisco inspirent une telle migration :CSCdr11146 (clients enregistrés uniquement)CSCdp18572 (clients enregistrés uniquement)CSCds40806 (clients enregistrés uniquement)

Q.Mon utilisation du CPU est élevée au niveau d'interruption, et je reçois des vidages si j'essaie un journal show. Le débit de trafic est également légèrement supérieur à la normale. Quelle en est la raison ?

A. Voici un exemple de la sortie de commande **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
```

Vérifiez si vous vous connectez à la console. Si oui, vérifiez s'il y a des requêtes HTTP de trafic. Ensuite, vérifiez s'il existe des listes d'accès avec des mots clés de journal ou des débogages qui

observent des flux IP particuliers. Si les vidages augmentent, c'est peut-être parce que la console, généralement un périphérique de 9 600 bauds, ne peut pas gérer la quantité d'informations reçues. Dans ce scénario, le routeur désactive les interruptions et ne traite que les messages de console. La solution consiste à désactiver la journalisation de console ou à supprimer le type de journalisation que vous effectuez.

Q. Je vois de nombreuses tentatives de connexion HTTP sur mon routeur IOS qui exécute un serveur ip http. Est-ce à cause de l'analyse du ver « Code Red » ?

R. « Code Red » peut être la raison ici. Cisco vous recommande de désactiver la commande **ip http server** sur le routeur IOS afin qu'il n'ait pas besoin de traiter de nombreuses tentatives de connexion d'hôtes infectés.

Solutions

Il y a différentes solutions qui sont discutées dans la section Avis qui discute du ver « Code Red ». Reportez-vous aux conseils pour connaître les solutions de contournement.

Une autre méthode pour bloquer le ver « Code Red » aux points d'entrée réseau utilise la reconnaissance NBAR (Network-Based Application Recognition) et les listes de contrôle d'accès (ACL) dans le logiciel IOS sur les routeurs Cisco. Utilisez cette méthode conjointement avec les correctifs recommandés pour les serveurs IIS de Microsoft. Pour plus d'informations sur cette méthode, référez-vous à Utilisation de NBAR et ACL pour bloquer le ver « Code Red » aux points d'entrée réseau.

Informations connexes

- Dépannage des problèmes de mémoire
- Dépannage des fuites de mémoire tampon
- Dépannage de l'utilisation élevée du CPU sur les routeurs Cisco
- Résolution des problèmes de blocage de routeurs
- Notes techniques de dépannage - Routeurs
- Dépannage du routeur
- Support et documentation techniques - Cisco Systems