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

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Comment le ver de « Code Red » infecte d'autres systèmes
Bulletins de renseignements qui discutent le ver de « Code Red »
Symptômes
Identifiez le périphérique infecté
Techniques de prévention
Le trafic de bloc au port 80
Réduisez l'utilisation mémoire d'entrée ARP
Changement de Technologie Cisco Express Forwarding (CEF) d'utilisation
Cisco Express Forwarding contre la commutation rapide
Comportement et implications de commutation rapide
Avantages de CEF
Exemple de sortie : CEF
Choses à considérer
Forums aux questions de « Code Red » et leurs réponses
Q. J'utilise NAT, et éprouve 100 pour cent d'utilisation du processeur dans l'IP Input. Quand j'exécute la CPU de show proc, mon utilisation du processeur est élevée dans le niveau de priorité d'interruption - 100/99 ou 99/98. Est-ce que ceci peut être lié au « Code Red » ?
Q. I exécutent IRB, et rencontrent l'utilisation du CPU élevé dans le processus d'entrée HyBridge. Que se passe-t-il ? Est relatif aux TI au « Code Red » ?
L'utilisation du processeur Q.My est élevée au niveau de priorité d'interruption, et je reçois des annulations si j'essaye un show log. Le débit de trafic est également seulement en quelque sorte normale de supérieur à. Quelle est la raison pour ceci ?
Q. Je peux voir de nombreuses tentatives de connexion HTTP sur mon routeur IOS qui exécute un ip http server. Est-ce que c'est en raison du balayage de ver de « Code Red » ?
Contournements
Informations connexes

Introduction

Ce document décrit le ver de « Code Red » et les problèmes que le ver peut poser à Cisco

conduisant l'environnement. Ce document également décrit des techniques pour empêcher l'infestation du ver et fournit des liens aux bulletins de renseignements relatifs qui décrivent des solutions pour des problèmes liés au ver.

Le ver de « Code Red » exploite une vulnérabilité dans le service d'index de la version 5.0 de Microsoft Internet Information Server (IIS). Quand le ver de « Code Red » infecte un hôte, il fait sonder et infecter l'hôte une gamme aléatoire d'adresses IP, qui entraîne une hausse forte du trafic réseau. C'est particulièrement problématique s'il y a des liens redondants dans le réseau et/ou le Technologie 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.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

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

Les tentatives de ver de « Code Red » de se connecter aux adresses IP aléatoirement générées. Chaque serveur infecté IIS peut tenter d'infecter le même ensemble de périphériques. Vous pouvez tracer l'adresse IP source et le port TCP du ver parce qu'il n'est pas charrié. Le Fonction Unicast Reverse Path Forwarding (uRPF) ne peut pas supprimer une attaque de ver parce que l'adresse source est juridique.

Bulletins de renseignements qui discutent le ver de « Code Red »

Ces bulletins de renseignements décrivent le ver de « Code Red », et expliquent comment corriger le logiciel affecté par le ver :

- Avis de sécurité Cisco : Ver de « Code Red » - Impact pour les clients
- Buffer Overflow distant d'extension ISAPI du serveur d'index IIS
- ver de « Code Red » .ida
- CERT ? Ver de « Code Red » du bulletin de renseignements CA-2001-19 exploitant le Buffer

Overflow dans le DLL de service d'indexation IIS

Symptômes

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

- Grand nombre d'écoulements dans les tables NAT ou de PAT (si vous utilisez NAT ou PAT).
- Le grand nombre de demandes d'ARP ou d'ARP fulmine dans le réseau (provoqué par le balayage d'adresse IP).
- Utilisation excessive de mémoire d'IP Input, d'entrée d'ARP, d'IP Cache Ager et de processus de CEF.
- Utilisation du CPU élevé dans l'ARP, l'IP Input, le CEF et l'IPC.
- Utilisation du CPU élevé au niveau de priorité d'interruption aux débits à faible trafic, ou utilisation du CPU élevé au niveau de processus dans l'IP Input, si vous utilisez NAT.

Un état de taille mémoire basse ou une utilisation du CPU élevé soutenue (100 pour cent) au niveau de priorité d'interruption peut faire recharger un routeur de Cisco IOS®. La recharge est provoqué par par un processus qui se conduit mal en raison des conditions d'effort.

Si vous ne suspectez pas que des périphériques dans votre site soient infectés par ou soient la cible du ver de « Code Red », voyez la section Informations connexes pour l'URLs supplémentaire sur la façon dont dépanner toutes les questions que vous rencontrez.

Identifiez le périphérique infecté

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

Après quelques minutes, émettez la commande de show ip cache flow de visualiser les entrées enregistrées. Pendant la phase initiale de l'infection de ver de « Code Red », les essais de ver pour se répliquer. La réplication se produit quand le ver envoie des demandes HT aux adresses IP aléatoires. Par conséquent, vous devez rechercher des entrées de flux de cache avec la destination port 80 (HT., 0050 dans l'hexa).

Le show ip cache flow | incluez 0050 que la commande affiche tout le cache entries avec un port TCP 80 (0050 dans l'hexa) :

```
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 anormalement un nombre élevé d'entrées avec la mêmes adresse IP source, adresse IP aléatoire[1 de] destination, DstP = 0050 (HTTP), et RP = 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 VLAN1.

la version [1Another du] ver de « Code Red », appelée le « Code Red II », ne choisit pas une adresse

IP totalement aléatoire de destination. Au lieu de cela, le « Code Red II » garde la partie réseau de l'adresse IP, et choisit une partie hôte aléatoire de l'adresse IP afin de propager. Ceci permet au ver pour se propager plus rapide dans le même réseau.

Le « 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)
```

Visez les adresses IP qui sont exclues sont 127.X.X.X et 224.X.X.X, et aucun octet n'est permis pour être 0 ou 255. En outre, l'hôte ne tente pas re-de s'infecter.

Le pour en savoir plus, se rapportent au Code Red (ii) .

Parfois, vous ne pouvez pas exécuter le NetFlow pour détecter une tentative d'infestation de « Code Red ». Ceci peut être parce que vous exécutez une version du code qui ne prend en charge pas le NetFlow, ou parce que le routeur a insuffisant ou mémoire excessivement fragmentée pour activer le NetFlow. Cisco recommande que vous n'activiez pas le NetFlow quand il y a de plusieurs interfaces d'entrée et seulement une interface de sortie sur le routeur, parce que la Fonction Netflow Accounting est exécutée sur le chemin d'entrée. Dans ce cas, il vaut mieux d'activer l'ip accounting sur l'interface de sortie solitaire.

Remarque: La commande d'ip accounting désactive DCEF. N'activez pas l'ip accounting sur aucune plate-forme où vous voulez 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 la sortie de commande de show ip accounting, recherchez les adresses sources qui tentent d'envoyer des paquets à de plusieurs adresses de destination. Si l'hôte infecté a lieu pendant la phase de balayage, il tente d'établir des connexions HTTP à d'autres Routeurs. Ainsi vous verrez des tentatives d'atteindre de plusieurs adresses IP. La majeure partie d'échouer de ces tentatives de connexion normalement. Par conséquent, vous voyez seulement un nombre restreint 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.

Quand vous exécutez le Commutation multicouche (MLS) sur la gamme Catalyst 5000 et la gamme Catalyst 6000, vous devez prendre différentes mesures pour activer la Fonction Netflow Accounting et pour dépister l'infestation. Dans un Cat6000 commutez équipé de la carte de commutation multicouche du superviseur 1 (MSFC1) ou SOUPEZ I/MSFC2, MLS basé sur NetFlow est activé par défaut, mais l'écoulement-mode est destination destination. Par conséquent, l'adresse IP source n'est pas cachée. Vous pouvez permettre au mode « à plein régime » de dépister les hôtes infectés avec l'aide de la pleine commande de set mls flow sur le superviseur.

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

```
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 commande d'IP de mls flow la pleine :

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

Quand vous activez le mode « à plein régime », un avertissement est affiché d'indiquer une augmentation très importante dans les entrées MLS. L'incidence des entrées MLS accrues est justifiable pour une durée si votre réseau est déjà infesté avec le ver de « Code Red ». Le ver rend vos entrées MLS excessives et sur l'arrivée.

Pour visualiser les informations collectées, utilisez ces commandes :

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

```
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 commande d'**IP de mls flow la pleine** :

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

Quand vous activez le mode « à plein régime », un avertissement est affiché d'indiquer une augmentation très importante dans les entrées MLS. L'incidence des entrées MLS accrues est justifiable pour une durée si votre réseau est déjà infesté avec le ver de « Code Red ». Le ver rend vos entrées MLS excessives et sur l'arrivée.

Pour visualiser les informations collectées, utilisez ces commandes :

Pour le mode hybride, utilisez la commande oto-rhino de show mls :

```
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 --------------- --------------- ----- -----
- ------ ----------------- ---- ---- ---- --------- --------- ---------- ----------- -------- --
------
```

Remarque: Tous ces champs sont complétés quand ils sont en mode « à plein régime ».

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

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

Quand vous déterminez l'adresse IP source et la destination port impliquées dans l'attaque, vous pouvez set mls de nouveau au mode « destination destination ».

Pour l'usage de mode hybride la commande de destination de set mls flow :

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

Pour le mode IOS natif, utilisez la commande de **destination d'IP de** mls flow :

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

La combinaison II/MSFC2 de superviseur (PETITE GORGÉE) est protégée contre l'attaque parce que la commutation de CEF est exécutée dans le matériel, et des statistiques Netflow sont mises à jour. Ainsi, même pendant une attaque de « Code Red », si vous activez le mode de flux complet, le routeur n'est pas inondé, en raison du mécanisme plus rapide de commutation. Les commandes d'activer le mode de flux complet et d'afficher les statistiques sont identiques sur la PETITE GORGÉE I/MFSC1 et la PETITE GORGÉE II/MSFC2.

Techniques de prévention

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

Le trafic de bloc au port 80

S'il est faisable dans votre réseau, le moyen le plus simple d'empêcher l'attaque de « Code Red » est de bloquer tout le trafic au port 80, qui est le port connu pour WWW. Établissez une liste d'accès pour refuser des paquets IP destinés au port 80 et pour les appliquer d'arrivée sur l'interface qui fait face à la source d'infection.

Réduisez l'utilisation mémoire d'entrée ARP

L'entrée d'ARP épuise des montants considérables de mémoire quand des points d'acheminement statiques à une interface de diffusion, comme ceci :

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

Chaque paquet pour le default route est envoyé au VLAN3. Cependant, il n'y a aucune prochaine adresse IP de saut spécifiée, et ainsi, le routeur envoie une demande d'ARP de l'adresse IP de destination. Le routeur du prochain saut pour cette destination répond avec sa propre adresse MAC, à moins que le proxy ARP soit désactivé. La réponse du routeur crée une entrée supplémentaire dans la table ARP où l'adresse IP de destination du paquet est tracée à l'adresse MAC de prochain-saut. Le ver de « Code Red » envoie des paquets aux adresses IP aléatoires, qui ajoute une nouvelle entrée d'ARP pour chaque adresse de destination aléatoire. Chaque nouvelle entrée d'ARP consomme de plus en plus la mémoire sous le processus d'entrée d'ARP.

Ne créez pas une route statique par défaut à une interface, particulièrement si l'interface est l'émission (Ethernet/Ethernet/GE/SMDS rapide) ou multipoint (vue Relay/ATM). N'importe quelle route statique par défaut doit indiquer l'adresse IP du routeur du prochain saut. Après que vous changiez le default route pour indiquer la prochaine adresse IP de saut, utilisez la commande de **clear arp-cache** d'effacer toutes les entrées d'ARP. Cette commande répare le problème d'utilisation de mémoire.

Changement de Technologie Cisco Express Forwarding (CEF) d'utilisation

Afin de diminuer l'utilisation du processeur sur un routeur IOS, modification de rapide/d'optimum/de Commutation Netflow à la commutation de CEF. Il y a quelques mises en garde pour activer le CEF. La section suivante discute la différence entre le CEF et la commutation rapide, et explique les implications quand vous activez le CEF.

Cisco Express Forwarding contre la commutation rapide

Permettez au CEF d'alléger le chargement d'augmentation du trafic provoqué par le ver de « Code Red ». Versions logicielles de Cisco IOS® 11.1 () cc, 12.0, et CEF postérieur de support sur les Plateformes de Cisco 7200/7500/GSR. Le soutien du CEF sur d'autres Plateformes est disponible dans Logiciel Cisco IOS version 12.0 ou plus tard. Vous pouvez étudier plus plus loin avec l'outil Software Advisor.

Parfois, vous ne pouvez pas activer le CEF sur tous les Routeurs dus à une de ces raisons :

- Mémoire insuffisante

- Architectures non vérifiées de plate-forme
- Encapsulations d'interface non prise en charge

Comportement et implications de commutation rapide

Voici les implications quand vous utilisez la commutation rapide :

- Cache piloté par trafic — Le cache est vide jusqu'à ce que le routeur commute des paquets et remplisse cache.
- Le premier paquet est commuté par processus — Le premier paquet est commuté par processus, parce que le cache est au commencement vide.
- Cache granulaire — Le cache est établi à une finesse de la pièce d'entrée de Routing Information Base la plus spécifique (NERVURE) d'un réseau principal. Si la NERVURE a /24s pour le réseau principal 131.108.0.0, le cache est établi avec /24s pour ce principal réseau.
- le cache de /32 est utilisé — le cache de /32 est utilisé pour équilibrer le chargement pour chaque destination. Quand le cache équilibre le chargement, le cache est établi avec /32s pour ce réseau principal.**Remarque:** Ces deux dernières questions peuvent potentiellement entraîner un cache énorme qui consommerait toute la mémoire.
- Mise en cache aux limites du réseau importantes — Avec le default route, cachant est exécuté aux limites du réseau importantes.
- L'ager de cache — L'ager de cache exécute chaque minute et vérifie le 1/20th (5 pour cent) du cache pour les entrées inutilisées dans des conditions normales de mémoire, et 1/4 (25 pour cent) du cache dans un état de taille mémoire basse (200k).

Afin de changer les valeurs ci-dessus, utilisez la commande **DE X/Y du cache-ager-intervalle Z d'IP**, où :

- X est nombre <0-2147483> de secondes entre les passages d'ager. Par défaut = 60 secondes.
- Y est <2-50> 1/(Y+1) du cache à vieillir par passage (mémoire basse). Par défaut = 4.
- Z est <3-100> 1/(Z+1) du cache à vieillir par passage (normal). Par défaut = 20.

Voici une configuration d'échantillon qui utilise le cache-**ager d'IP 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
```

Basé sur la configuration de votre ager de cache, un certain pourcentage de votre âge de cache entries hors de votre table de cache rapide. Quand l'âge d'entrées 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 réduit. Un inconvénient est que le trafic continue à circuler pour les entrées qui ont été vieillies hors de la table de cache. Les paquets initiaux sont commutés par processus, qui entraîne un pic court dans la consommation CPU dans l'**IP Input** jusqu'à ce qu'une nouvelle entrée de cache soit établie pour l'écoulement.

Des versions du logiciel Cisco IOS 10.3(8), 11.0(3) et plus tard, l'ager de cache IP est manipulé différemment, comme expliqué ici :

- **Le cache-ager-intervalle d'IP** et les commandes d'**ip cache-invalidate-delay** sont disponibles seulement si la commande **interne de service** est définie dans la configuration.
- Si la période entre les passages d'invalidation d'ager est fixée à 0, le processus d'ager est désactivé entièrement.
- Le temps est exprimé en quelques secondes.

Remarque: Quand vous exécutez ces commandes, l'utilisation du processeur du routeur augmente. Utilisez ces commandes seulement si 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 de CEF

- La table de Forwarding Information Base (FIB) est construite a basé sur la table de routage. Par conséquent les informations d'expédition existent avant que le premier paquet soit expédié. Le FIB contient également des entrées de /32 pour les hôtes directement connectés de RÉSEAU LOCAL.
- La table de la contiguïté (réglage) contient les informations de réécriture de la couche 2 pour des prochain-sauts et des hôtes direct-connectés (une entrée d'ARP crée une contiguïté CEF).
- Il n'y a aucun concept d'ager de cache avec le CEF pour clouer l'utilisation du processeur. Une entrée de FIB est supprimée si une entrée de table de routage est supprimée.

Attention : De nouveau, un default route qui indique une émission ou une interface multipoint signifie que le routeur envoie des demandes d'ARP de chaque nouvelle destination. Les demandes d'ARP du routeur créent potentiellement une table de juxtaposition énorme jusqu'au routeur manque de mémoire. Si le CEF n'alloue pas la mémoire CEF/DCEF se désactive. Vous devrez activer manuellement le CEF/DCEF de nouveau.

Exemple de sortie : CEF

Voici une certaine sortie témoin de la commande de show ip cef summary, cette utilisation de mémoire d'expositions. Cette sortie est un instantané d'un serveur de route de 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
```

Choses à considérer

Quand le nombre d'écoulements est grand, le CEF consomme typiquement moins de mémoire que la commutation rapide. Si la mémoire est déjà consommée par un cache de commutation rapide, vous devez effacer le cache d'ARP (par la commande de **clear ip arp**) avant que vous activiez le CEF.

Remarque: Quand vous effacez le cache, un pic est provoqué par dans l'utilisation du processeur du routeur.

Forums aux questions de « Code Red » et leurs réponses

Q. J'utilise NAT, et éprouve 100 pour cent d'utilisation du processeur dans l'IP Input. Quand j'exécute la CPU de show proc, mon utilisation du processeur est élevée dans le niveau de priorité d'interruption - 100/99 ou 99/98. Est-ce que ceci peut être lié au « Code Red » ?

R. Là récemment est réparé une bogue Cisco NAT (CSCdu63623 (clients enregistrés seulement)) qui implique l'évolutivité. Quand il y a des dizaines de milliers d'écoulements NAT (basés sur le type de plate-forme), la bogue entraîne 100 pour cent d'utilisation du processeur au niveau de priorité d'interruption de processus ou.

Afin de déterminer si cette bogue est la raison, émettez la commande align d'**exposition**, et la vérifiez si le routeur fait face à des erreurs de cadrage. Si vous voyez des erreurs ou des accès mémoire erratiques de cadrage, émettez la commande align d'**exposition** quelques fois et voyez si les erreurs sont sur l'arrivée. Si le nombre d'erreurs est sur l'arrivée, les erreurs de cadrage peuvent être la cause de l'utilisation du CPU élevé au niveau de priorité d'interruption, et pas la bogue Cisco CSCdu63623 (clients enregistrés seulement). Le pour en savoir plus, se rapportent à des accès erratiques de dépannage et à des erreurs de cadrage.

La commande **nat de traduction de show ip** affiche le nombre de traductions actives. Le point de fusion pour un processeur de la classe NPE-300 est environ 20,000 à 40,000 traductions. Ce nombre varie basé sur la plate-forme.

Ce problème de fusion a été observé précédemment par quelques clients, mais après « Code Red », plus de clients ont rencontré ce problème. Le seul contournement est d'exécuter NAT (au lieu de PAT), de sorte qu'il y ait moins traductions actives. Si vous avez des 7200, utilisez un NSE-1, et diminuez les valeurs du dépassement de durée NAT.

Q. I exécutent IRB, et rencontrent l'utilisation du CPU élevé dans le processus d'entrée HyBridge. Que se passe-t-il ? Est relatif aux TI au « Code Red » ?

R. Le processus d'entrée HyBridge manipule tous les paquets qui ne peuvent pas être à commutation rapide par le processus IRB. L'incapacité du rapide-commutateur de processus IRB un paquet peut être parce que :

- Le paquet est un paquet d'émission.
- Le paquet est un paquet de multidiffusion.
- La destination est inconnue, et l'ARP doit être déclenché.
- Il y a le spanning-tree BPDU.

Le HyBridge Input rencontre des problèmes s'il y a des milliers d'interfaces point par point dans le même groupe de passerelle. Le HyBridge Input rencontre également des questions (mais dans une moindre mesure) s'il y a des milliers de VSs dans la même interface multipoint.

Quels sont des possibles raison pour des problèmes avec IRB ? Supposez qu'un périphérique infecté par le « rouge de code » balaye des adresses IP.

- Le routeur doit envoyer une demande d'ARP de chaque adresse IP de destination. Une pléthore d'ARP demande le résultat sur chaque circuit virtuel dans le groupe de passerelle pour chaque adresse qui est balayée. Le processus normal d'ARP ne pose pas un problème CPU. Cependant, s'il y a une entrée d'ARP sans entrée de passerelle, le routeur inonde des paquets destinés pour les adresses pour lesquelles les entrées d'ARP existent déjà. Ceci peut entraîner l'utilisation du CPU élevé parce que le trafic est commuté par processus. Pour éviter le problème, augmenter l'heure de passerelle-vieillissement (par défaut 300 secondes ou 5 minutes) d'apparier ou dépasser le délai d'attente d'ARP (par défaut 4 heures) de sorte que les infidèles soient synchronisés.
- L'adresse que l'hôte d'extrémité tente d'infecter est une adresse d'émission. Le routeur fait l'équivalent d'une diffusion de sous-réseau qui doit être répliquée par le processus d'entrée HyBridge. Ceci ne se produit pas si l'**aucune** commande d'**ip directed-broadcast** n'est configurée. Du Logiciel Cisco IOS version 12.0, la commande d'**ip directed-broadcast** est désactivée par défaut, qui cause toutes les émissions IP-dirigées d'être abandonnées.
- Voici une note marginal, indépendante du « Code Red », et connexe aux architectures IRB :Des paquets de Multidiffusion et d'émission de la couche 2 doivent être répliqués. Par conséquent, un problème avec les serveurs IPX qui fonctionnent sur un segment de diffusion peut réduire le lien. Vous pouvez employer des stratégies d'abonné pour éviter le problème. Le pour en savoir plus, se rapportent au Fonction x Digital Subscriber Line (xDSL) Bridge Support. Vous devez également considérer les Listes d'accès de passerelle, qui limitent le type de trafic permis pour traverser le routeur.
- Afin d'alléger ce problème IRB, vous pouvez utiliser des plusieurs groupes de ponts, et vous assurez qu'il y a un mappage linéaire pour BVIs, des sous-interfaces et VCs.
- RBE est supérieur à IRB parce qu'il évite la pile traversière totalement. Vous pouvez migrer vers RBE d'IRB. Ces bogues Cisco inspirent un tel transfert :CSCdr11146 (clients enregistrés seulement)CSCdp18572 (clients enregistrés seulement)CSCds40806 (clients enregistrés seulement)

L'utilisation du processeur Q.My est élevée au niveau de priorité d'interruption, et je reçois des annulations si j'essaye un show log. Le débit de trafic est également seulement en quelque sorte normale de supérieur à. Quelle est la raison pour ceci ?

R. Voici un exemple de la sortie de commande de **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 demandes de HTTP du trafic. Ensuite, le contrôle s'il y a des Listes d'accès avec des mots clé de journal ou met au point que l'IP particulier de montre circule. Si les annulations sont sur l'arrivée, elle peut être parce que la console, habituellement un périphérique de 9600 bauds, ne peut pas manipuler la quantité d'informations reçue. Dans ce scénario, les interruptions de débronchements de routeur et fait des messages console de rien mais de processus. La solution est de désactiver la journalisation console ou d'enlever Qu'est ce que type de se connecter vous exécutez.

Q. Je peux voir de nombreuses tentatives de connexion HTTP sur mon routeur IOS qui exécute un ip http server. Est-ce que c'est en raison du balayage de ver de « Code Red » ?

A. « Code Red » peut être la raison ici. Cisco recommande que vous désactiviez la commande d'**ip http server** sur le routeur IOS de sorte qu'elle n'ait pas besoin de traiter de nombreuses tentatives de connexion des hôtes infectés.

Contournements

Il y a de divers contournements qui sont discutés dans les bulletins de renseignements qui discutent la section de ver de « Code Red ». Référez-vous aux bulletins de renseignements pour les contournements.

Une autre méthode pour bloquer le ver de « Code Red » aux points d'entrée du réseau utilise le Reconnaissance d'application fondée sur le réseau (NBAR) et le Listes de contrôle d'accès (ACL) dans le logiciel IOS sur des Routeurs de Cisco. Utilisez cette méthode en même temps que les correctifs recommandés pour des serveurs IIS de Microsoft. Pour plus d'informations sur cette méthode, référez-vous en utilisant NBAR et ACLs pour bloquer le ver de « Code Red » aux points d'entrée du 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
- Dépannage de TechNotes - Routeurs
- Dépannage du routeur
- Support et documentation techniques - Cisco Systems