Gebruik van mallocaten en hoge CPU's als gevolg van het "coderode" worm

Inhoud

Inleiding

Dit document beschrijft de "Rode" worm van de Code en de problemen die de worm in een Cisco Routing omgeving kan veroorzaken. In dit document worden ook technieken beschreven om besmetting van de worm te voorkomen en worden koppelingen naar verwante adviseurs gegeven

waarin oplossingen worden beschreven voor wormgerelateerde problemen.

De "Code Red" worm exploiteert een kwetsbaarheid in de Index Service van de Microsoft Internet Information Server (IS) versie 5.0. Wanneer de "Code Red" worm een host infecteert, veroorzaakt het dat de host wordt onderzocht en infecteert het een willekeurige reeks IP adressen, wat een scherpe stijging van het netwerkverkeer veroorzaakt. Dit is vooral problematisch als er redundante links in het netwerk zijn en/of Cisco Express Forwarding (CEF) wordt niet gebruikt om pakketten switches.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Hoe het "rode code"-werk andere systemen beïnvloedt

De worm "Code Red" probeert verbinding te maken met willekeurig gegenereerde IP adressen. Elke geïnfecteerde IS server kan proberen om dezelfde reeks apparaten te infecteren. U kunt het IP-adres van de bron en de TCP-poort van de worm overtrekken omdat deze niet is gespoofd. Unicast Reverse Path Forwarding (URPF) kan een wormaanval niet onderdrukken omdat het bronadres legaal is.

Advisories waarin het woord "rood" wordt besproken

Deze adviseurs beschrijven de "Code Red" worm en leggen uit hoe de software die door de worm wordt getroffen, kan worden geplakt:

- Cisco Security Advies: "Code Red" - effect van de klant
- Remote IS Index Server ISAPI-uitbreidingsbuffer
- .ida "Code Red" worm
- ZEKER? Advies CA-2001-19 "Code Red" worm Exploiting Buffer Overflow in IS Indexing Service DLL

Symptomen

Hier zijn enkele symptomen die erop duiden dat een Cisco-router wordt beïnvloed door de 'Code Red'-worm:

- Een groot aantal stromen in NAT- of PAT-tabellen (als u NAT of PAT gebruikt).
- Een groot aantal ARP-verzoeken of ARP-stormen in het netwerk (veroorzaakt door de IP-adresscan).
- Extreem geheugen gebruik door IP Input, ARP Input, IP Cache Ager en CEF processen.
- Gebruik van hoge CPU's in ARP, IP-ingangen, CEF en IPC.
- Gebruik van hoge CPU's op niveau van onderbreking bij lage verkeerssnelheden of gebruik van hoge CPU's op procesniveau in IP-ingangen, indien u NAT gebruikt.

Een toestand van laag geheugen of een duurzaam hoog CPU-gebruik (100%) op niveau van onderbreking kan een Cisco IOS®-router ertoe aanzetten opnieuw te laden. De herlading wordt veroorzaakt door een proces dat zich slecht gedraagt als gevolg van de stressomstandigheden.

Als u niet vermoedt dat apparaten in uw site geïnfecteerd zijn door of het doelwit zijn van de 'Code Red'-worm, zie de Gerelateerde informatie sectie voor extra URL's over hoe u problemen kunt oplossen die u tegenkomt.

Identificeer het besmette apparaat

Gebruik stroomomschakeling om het bron IP adres van het getroffen apparaat te identificeren. Configureer de **ip route-cache flow op alle interfaces om alle stromen op te nemen die door de router zijn geschakeld.**

Na een paar minuten geeft u de **opdracht tonen ip cache flow om de opgenomen items te bekijken.** Tijdens de eerste fase van de infectie met de "rode code" wormen, probeert de worm zichzelf te repliceren. De replicatie gebeurt wanneer de worm HT verzoeken naar willekeurige IP adressen stuurt. Daarom moet u zoeken naar cache flow-items met bestemmingpoort 80 (HT., 0050 in hex).

De **ip cache flow | inclusief 0050** commando geeft alle cache items weer met een TCP poort 80 (0050 in hex):

```
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
```

Als u een abnormaal hoog aantal items met hetzelfde bron-IP-adres, willekeurig doeladres[1], DstP = 0050 (HTTP) en Pr = 06 (TCP) vindt, hebt u waarschijnlijk een besmet apparaat gevonden. In dit

uitvoervoorbeeld, is het bron IP-adres 193.23.45.35 en komt van VLAN1.

[1] Een andere versie van de "Code Red"-worm, genaamd "Code Red II", kiest geen volledig willekeurig IP-adres. In plaats hiervan houdt "Code Red II" het netwerkgedeelte van het IP adres bij en kiest een willekeurig host-gedeelte van het IP-adres om te propageren. Hierdoor kan de worm zich sneller verspreiden binnen hetzelfde netwerk.

"Code Red II" gebruikt deze netwerken en maskers:

```
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)
```

Uitgesloten Target IP-adressen zijn 127.X.X.X en 224.X.X.X en er mag geen octet 0 of 255 zijn. Daarnaast probeert de host zichzelf niet opnieuw te infecteren.

Raadpleeg voor meer informatie Code Red (II) .

Soms kan je geen netflow gebruiken om een "Code Red" bebossingspoging te detecteren. Dit kan zijn omdat u een versie van code runt die geen netflow ondersteunt, of omdat de router onvoldoende of buitensporig gefragmenteerd geheugen heeft om netflow mogelijk te maken. Cisco raadt u aan geen netflow in te schakelen wanneer er meerdere ingangsinterfaces en slechts één ress interface op de router zijn, omdat de netwerkflow-accounting op het ingangspad wordt uitgevoerd. In dit geval is het beter om IP-accounting in de enige spanning interface mogelijk te maken.

Opmerking: de opdracht ip accounting schakelt DCEF uit. Laat IP accounting op geen enkel platform toe waar u DCEF-switching wilt gebruiken.

```
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
```

In de opdrachtoutput van ip accounting, zoek bronadressen die pakketten naar meerdere doeladressen proberen te verzenden. Als de geïnfecteerde host zich in de scanfase bevindt, probeert deze HTTP-verbindingen op te zetten met andere routers. U zult dus pogingen zien om meerdere IP adressen te bereiken. De meeste van deze verbindingspogingen mislukken

doorgaans. Daarom ziet u slechts een klein aantal overgebrachte pakketten, elk met een kleine byte-telling. In dit voorbeeld is het waarschijnlijk dat 20.1.145.49 en 20.1.104.194 besmet zijn.

Wanneer u Multi-Layer Switching (MLS) uitvoert op Catalyst 5000 Series en Catalyst 6000 Series, moet u verschillende stappen nemen om NetFlow-accounting mogelijk te maken en de vervuiling op te sporen. In een Cat6000 switch die is uitgerust met Supervisor 1 Multilayer Switch functiekaart (MSFC1) of SUP I/MSFC2, is op netflow gebaseerde MLS standaard ingeschakeld, maar de flow-mode is alleen op bestemming gericht. Daarom wordt het IP-adres van de bron niet gecached. U kunt de "full-flow" modus inschakelen om geïnfecteerde hosts op te sporen met behulp van de **ingestelde mls flow full**-opdracht van de toezichthouder.

Gebruik voor hybride modus de **ingestelde mls flow full**-opdracht:

```
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.
```

Voor Native IOS modus, gebruik de **mls flow ip volledig bevel:**

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

Wanneer u "full-flow" modus instelt, wordt er een waarschuwing weergegeven om een dramatische toename in MLS items aan te geven. De impact van de toegenomen MLS-vermeldingen is voor een korte periode te rechtvaardigen als uw netwerk al besmet is met de "Code Red" worm. De worm zorgt ervoor dat je MLS inzendingen excessief zijn en in opkomst.

U kunt de verzamelde informatie als volgt weergeven:

Gebruik voor hybride modus de **ingestelde mls flow full**-opdracht:

```
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.
```

Voor Native IOS modus, gebruik de **mls flow ip volledige** opdracht:

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

Wanneer u "full-flow" modus instelt, wordt er een waarschuwing weergegeven om een dramatische toename in MLS items aan te geven. De impact van de toegenomen MLS-vermeldingen is voor een korte periode te rechtvaardigen als uw netwerk al besmet is met de "Code Red" worm. De worm zorgt ervoor dat je MLS inzendingen excessief zijn en in opkomst.

U kunt de verzamelde informatie als volgt weergeven:

Voor Hybride modus gebruikt u de opdracht **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
```

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

N.B.: al deze velden zijn ingevuld wanneer ze in de "full-flow" modus staan.

Voor Native IOS modus, gebruik de opdracht **show mls ip**:

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

Wanneer u het bron IP-adres en de doelpoort bepaalt die bij de aanval betrokken zijn, kunt u MLS terugzetten naar de "bestemming-only" modus.

Gebruik voor hybride modus de **ingestelde mls flow bestemmingopdracht**:

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

Voor Native IOS-modus, gebruik de **mls flow ip**-opdracht:

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

De Supervisor (SUP) II/MSFC2 combinatie wordt beschermd tegen aanval omdat CEF omschakeling in de hardware wordt uitgevoerd, en de netflow statistiek wordt gehandhaafd. Zelfs tijdens een ‘Code Red' aanval, als u de Full-flow-modus toelaat, wordt de router niet ingeslikt door het snellere switching-mechanisme. De opdrachten om de volledige-stroommodus in te schakelen en de statistieken weer te geven, zijn dezelfde bij zowel SUP I/MFSC1 als bij SUP II/MSFC2.

Preventieve technieken

Gebruik de technieken in deze sectie om de impact van de "Code Rode"-worm op de router te minimaliseren.

Blokverkeer naar poort 80

Als dit op uw netwerk mogelijk is, is de makkelijkste manier om de "Code Red" aanval te voorkomen het hele verkeer naar poort 80 blokkeren, de bekende haven voor WW. Bouw een access-list om IP pakketten te ontkennen die voorbestemd zijn om te haven 80 toe te passen en het binnenkomend op de interface toe die de besmettingsbron onder ogen ziet.

Gebruik van ARP-invoergeheugen verminderen

ARP Input gebruikt grote hoeveelheden geheugen op wanneer een statische route naar een uitzending wijst, zoals deze:

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

Elk pakket voor de standaardroute wordt naar VLAN3 verzonden. Er is echter geen volgende opgegeven IP-adres van de hop en dus stuurt de router een ARP-verzoek naar het IP-adres van

de bestemming. De volgende hoprouter voor die bestemming antwoordt met zijn eigen adres van MAC, tenzij Proxy ARP uitgeschakeld is. Het antwoord van de router leidt tot een extra ingang in de ARP lijst waar het IP-adres van de bestemming van het pakket aan het volgende-hop adres van MAC in kaart wordt gebracht. De "Rode" worm van de Code stuurt pakketten naar willekeurige IP adressen, die een nieuwe ARP ingang voor elk willekeurig bestemmingsadres toevoegen. Elke nieuwe ARP-ingang verbruikt meer en meer geheugen onder het ARP-invoerproces.

Maak geen statische standaardroute naar een interface, vooral als de interface wordt uitgezonden (Ethernet/Fast Ethernet/GE/SMDS) of multipoint (Frame Relay/ATM). Elke statische standaardroute moet naar het IP-adres van de volgende hoprouter wijzen. Nadat u de standaardroute om naar het volgende hop-IP-adres te wijzen verandert, gebruikt u de **heldere arp-cache** opdracht om alle ARP-items te wissen. Deze opdracht vormt de oplossing voor het probleem met de geheugenbenutting.

Gebruik Cisco Express Forwarding (CEF)-switching

Om het gebruik van CPU op een IOS-router te verlagen, verandert u van Fast/Optimum/NetFlow-switching naar CEF. Er zijn een paar uitzonderingen om CEF mogelijk te maken. De volgende paragraaf bespreekt het verschil tussen CEF en fast switching en legt de implicaties uit wanneer je CEF toelaat.

Cisco Express Forwarding versus Fast Switching

CEF in staat stellen om de toegenomen verkeersbelasting die door de "Code Red"-worm wordt veroorzaakt, te verlichten. Cisco IOS®-softwarereleases 11.1(1)CC, 12.0 en hoger ondersteuning voor CEF op de Cisco 7200/7500/GSR-platforms. Ondersteuning voor CEF op andere platforms is beschikbaar in Cisco IOS-softwarerelease 12.0 of hoger. U kunt verder onderzoek doen met het Softwareadviseur.

Soms kunt u om een van deze redenen CEF op alle routers niet inschakelen:

- Onvoldoende geheugen
- Niet-ondersteunde platformarchitecturen
- Niet-ondersteunde interface-insluiting

Snel switchinggedrag en -implicaties

Hier zijn de implicaties wanneer je snel overstapt:

- Verkeersgedreven cache — Het cache is leeg tot de router switches en het cache opvult.
- Het eerste pakket is proces-switched - het eerste pakket is proces-geschakeld, omdat het cache aanvankelijk leeg is.
- Granulair cache—Het cache is gebouwd op een granulariteit van het meest specifieke routinginformatiemechanisme (RIB)-ingangsdeel van een groot net. Als RIB /24s heeft voor groot netto 131.108.0.0, is het cache gebouwd met 24s voor dit belangrijke netwerk.
- /32 cache wordt gebruikt—/32 cache wordt gebruikt om de lading voor elke bestemming in evenwicht te brengen. Als de cache-balans-lading oplevert, wordt de cache opgebouwd met /32s voor dat belangrijke net.**Opmerking:** Deze laatste twee problemen kunnen mogelijk een

groot cache opleveren dat alle geheugen zou verbruiken.
- Cacken bij grote netwerkgrenzen—Van standaardroute wordt het caching uitgevoerd bij grote netwerkgrenzen.
- De Cache Ager-The cache ager runt elke minuut en controleert 1/20th (5%) van de cache voor ongebruikte items onder normale geheugenomstandigheden en 1/4th (25%) van de cache in een lage geheugenconditie (200k).

Om de bovenstaande waarden te veranderen, gebruikt u de **ip cache-ager-interval X Y Z** opdracht, waarbij:

- X is <0-2147483> aantal seconden tussen tijdelijke instelling. Standaard = 60 seconden.
- Y is <2-50> 1/(Y+1) cache naar leeftijd per run (weinig geheugen). Standaard = 4.
- Z is <3-100> 1/(Z+1) cache naar leeftijd per run (normaal). Standaard = 20.

Hier is een voorbeeldconfiguratie die gebruikmaakt van **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
```

Gebaseerd op de instelling van je cache ager, een percentage van je cache items in de leeftijd van je fast-cache-tabel. Als de inzendingen snel ouder worden, wordt een groter percentage van de fast-cache tabelpagina's, en de cache tabel kleiner. Als resultaat hiervan vermindert de geheugenconsumptie op de router. Een nadeel is dat het verkeer blijft stromen voor de items die uit de cache-tabel zijn verouderd. Initiële pakketten zijn procesgeschakeld, wat een korte piek in CPU-verbruik in **IP** veroorzaakt tot een nieuwe cache-ingang voor de stroom is ingebouwd.

Van Cisco IOS-softwarereleases 10.3(8), 11.0(3) en later wordt de IP cache-gebruiker anders verwerkt, zoals hier wordt uitgelegd:

- De **ip cache-ager-interval** en **ip cache-invaliderende vertragingsopdrachten** zijn alleen beschikbaar als de **service interne** opdracht in de configuratie is gedefinieerd.
- Als de periode tussen de "ager"-geldigheidstermijn op 0 is ingesteld, wordt het "ager"-proces geheel uitgeschakeld.

- De tijd wordt uitgedrukt in seconden.

N.B.: Wanneer u deze opdrachten uitvoert, wordt het CPU-gebruik van de router verhoogd. Gebruik deze opdrachten alleen als dit absoluut nodig is.

```
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
```

Voordelen van CEF

- De tabel Forwarding Information Base (FIB) is gebaseerd op de routingtabel. Daarom bestaat het verzenden van informatie voordat het eerste pakket wordt doorgestuurd. Het FIB bevat ook /32 ingangen voor direct aangesloten LAN hosts.
- De ADJ-tabel (Adjacency) bevat Layer 2 om informatie te herschrijven voor de volgende hop en direct-verbonden hosts (een ARP-vermelding maakt een CEF-nabijheid).
- Er is geen cacheager concept met CEF om CPU-gebruik te versnellen. Een FIB-ingang wordt verwijderd als een routingtabelingang wordt verwijderd.

Waarschuwing: Opnieuw, een standaardroute die naar een uitzending of multipoint interface wijst betekent dat de router ARP verzoeken voor elke nieuwe bestemming stuurt. ARP verzoeken van de router creëren potentieel een grote nabijheidslijst tot de router uit het geheugen loopt. Als CEF er niet in slaagt het geheugen CEF/DCEF toe te wijzen, schakelt het zichzelf uit. U dient CEF/DCEF opnieuw handmatig in te schakelen.

Uitvoer van monster: CEF

Hier is een aantal voorbeelduitvoer van de opdracht samenvatting van **het ip cef**, die geheugengebruik toont. Deze uitvoer is een snapshot van een Cisco 7200 routeserver met Cisco IOS-softwarerelease 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
```

Te overwegen dingen

Wanneer het aantal stromen groot is, gebruikt CEF doorgaans minder geheugen dan snelle switching. Als geheugen al geconsumeerd wordt door een snelle switching cache moet u het ARP cache verwijderen (door het **heldere ip arp** opdracht) voordat u CEF in staat stelt.

Opmerking: Wanneer u het cache opheft, wordt een piek veroorzaakt in het CPU-gebruik van de router.

"Code Red" Vaak gestelde vragen en hun antwoorden

Q. Ik gebruik NAT en ervaart 100 procent CPU-gebruik in IP-ingangen. Wanneer ik een toonproc cpu uitvoert, is mijn CPU-gebruik hoog in interrupt niveau - 100/99 of 99/98. Kan dit gerelateerd zijn aan "Code Red"?

A. Er is onlangs een NAT Cisco bug (CSCdu63623 (alleen geregistreerde klanten)) die schaalbaarheid impliceert. Wanneer er tienduizenden NAT-stromen zijn (gebaseerd op het platform), veroorzaakt de bug een gebruik van 100 procent CPU's tijdens het proces of wordt het niveau onderbroken.

Om te bepalen of deze bug de reden is, geeft u de **show uitlijning** opdracht uit en controleert u of de router uitlijning fouten tegenkomt. Als u uitlijning fouten of foutieve geheugentoegang ziet, geeft u de **show** opdrachtregel een paar keer uit en ziet u of de fouten in opkomst zijn. Als het aantal fouten toeneemt, kunnen uitlijning fouten de oorzaak zijn van een hoog CPU-gebruik op niveau van onderbreking en niet Cisco bug CSCdu63623 (alleen geregistreerde klanten). Raadpleeg voor meer informatie de foutmelding van probleemoplossing bij onduidelijke toegang en uitlijning.

De **show ip nat translatie** opdracht toont het aantal actieve vertalingen. Het meltdown-punt voor een NPE-300-klasse processor is ongeveer 20.000 tot 40.000 vertalingen. Dit aantal varieert op basis van het platform.

Dit meltdown-probleem werd eerder door een paar klanten gezien, maar na "Code Red" hebben meer klanten dit probleem ervaren. Het enige alternatief is om NAT (in plaats van PAT) te gebruiken, zodat er minder actieve vertalingen zijn. Als u een 7200 hebt, gebruikt u een NSE-1 en verlaagt u de NAT timeout waarden.

Q. Ik voer IRB uit en ontmoet een hoog CPU-gebruik in het HyBridge Input-proces. Waarom gebeurt dit? Is het gerelateerd aan "Code Red"?

A. Het HyBridge Input-proces verwerkt alle pakketten die niet snel kunnen worden geschakeld met het IRB-proces. Het onvermogen van het IRB-proces om een pakket snel te switches kan zijn omdat:

- Het pakket is een uitzending.
- Het pakket is een multicast pakket.
- De bestemming is onbekend en ARP moet worden geactiveerd.
- Er overspannen drie BPDU's.

De HyBridge Inv ontmoet problemen als er duizenden point-to-point interfaces in dezelfde bridge groep zijn. HyBridge Input ontmoet ook problemen (maar in mindere mate) als er duizenden VS's zijn in dezelfde multipoint interface.

Wat zijn de mogelijke redenen voor problemen met IRB? Stel dat een apparaat dat is besmet met "Code red" IP-adressen scant.

- De router moet een ARP verzoek voor elk bestemming IP adres verzenden. Een vloed van ARP verzoeken resultaat bij elke VC in de bridge groep voor elk adres dat gescand wordt. Het

normale ARP-proces veroorzaakt geen CPU-probleem. Als er echter een ARP-vermelding zonder bridge is, worden de routers overstromingen voorzien van adressen waarvoor reeds ARP-vermeldingen bestaan. Dit kan een hoog CPU-gebruik veroorzaken omdat het verkeer naar een andere computer wordt overgeschakeld. Om het probleem te vermijden, verhoog de bridge-verouderingstijd (standaard 300 seconden of 5 minuten) om de ARP timeout (standaard 4 uur) aan te passen of te overschrijden zodat de twee timers gesynchroniseerd zijn.

- Het adres dat de eindgastheer probeert te infecteren is een uitzending adres. De router doet het equivalent van een netto uitzending die door het proces van de Invoer van de HyBridge moet worden gerepliceerd. Dit gebeurt niet als de opdracht **geen ip**, **gericht-uitzending** is ingesteld. Van Cisco IOS-softwarerelease 12.0 wordt de opdracht **ip** gericht-uitzending standaard uitgeschakeld, waardoor alle IP-gerichte uitzendingen vallen.
- Hier is een briefje dat niets te maken heeft met "Code Red" en betrekking heeft op IRB-architecturen:Layer 2 multicast en broadcast moeten worden gerepliceerd. Daarom kan een probleem met IPX-servers die op een uitzending-segment lopen de link naar beneden brengen. U kunt het abonneebeleid gebruiken om het probleem te voorkomen. Raadpleeg voor meer informatie de xDSL-bridge (x Digital Subscriber Line). U moet ook overbruggingstoegangslijsten overwegen, die het type verkeer beperken dat door de router wordt toegestaan door te gaan.
- Om dit IRB-probleem te verhelpen, kunt u meerdere bruggroepen gebruiken en ervoor zorgen dat er één-op-één-omzetting is voor BVI's, subinterfaces en VC's.
- RBE is beter dan IRB, omdat zij de overbruggingsstack geheel vermijdt. Je kunt migreren naar RBE van IRB. Deze Cisco-insecten inspireren dergelijke migratie:CSCdr1146 (alleen geregistreerde klanten)CSCdp18572 (alleen geregistreerde klanten)CSCds40806 (alleen geregistreerde klanten)

Q.Mijn CPU-gebruik is hoog op niveau van onderbreking, en ik krijg flushes als ik een showlogbestand probeer. Het verkeerspercentage is ook iets hoger dan normaal. Wat is de reden hiervoor?

A. Hier is een voorbeeld van de opdrachtoutput **van 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
```

Controleer of u logt naar de console. Als dit zo is, controleer of er verzoeken zijn van HTTP van het verkeer. Controleer vervolgens of er toegangslijsten zijn met zoekwoorden of knoppen die op bepaalde IP-stromen letten. Als flushes stijgen kan het zijn omdat de console, meestal een 9600 basisapparaat, niet in staat is om de hoeveelheid ontvangen informatie te verwerken. In dit scenario schakelt de router onderbrekingen uit en verwerkt niets behalve consoleboodschappen. De oplossing is om console houtkap uit te schakelen of elk type houtkap te verwijderen dat u uitvoert.

Q. Ik kan talloze HTTP connectie pogingen zien op mijn IOS router die een ip http-server runt. Is dit vanwege de "Code Red" worm scan?

A. "Code Red" kan hier de reden zijn. Cisco raadt u aan om de opdracht **ip http server** op de IOS router uit te schakelen zodat deze niet met talrijke verbindingspogingen van geïnfecteerde hosts hoeft te worden behandeld.

zorgwekkende

In de Advisories worden verschillende discussies besproken over het onderdeel "Code Red". Raadpleeg de adviezen voor het omgaan met problemen.

Een andere methode om de "Code Red" worm op netwerkingspunten te blokkeren gebruikt Network-Based Application Recognition (NBAR) en Access Control Lists (ACL's) binnen IOS-software op Cisco-routers. Gebruik deze methode in combinatie met de aanbevolen patches voor IIS-servers van Microsoft. Raadpleeg voor meer informatie over deze methode NBAR en ACL's gebruiken om het "Code Red"-werk bij Network Ingress Point te blokkeren.

Gerelateerde informatie

- Problemen oplossen
- Buffer-lekken voor probleemoplossing
- Gebruik van hoge CPU's voor probleemoplossing op Cisco-routers
- Routercrashes voor probleemoplossing
- TechNotes voor probleemoplossing - routers
- Problemen oplossen
- Technische ondersteuning en documentatie – Cisco Systems