Umgang mit Mallocfail und hoher CPU-Auslastung durch den Wurm "Code Red"

Inhalt

Einführung

Dieses Dokument beschreibt den "Code Red" Wurm und die Probleme, die der Wurm in einer Cisco Routing-Umgebung verursachen kann. Dieses Dokument beschreibt außerdem Techniken zur Verhinderung des Befalls des Wurms und enthält Links zu entsprechenden Ratgebern, die

Lösungen für Probleme im Zusammenhang mit Würmern beschreiben.

Der Wurm "Code Red" nutzt eine Schwachstelle im Index Service von Microsoft Internet Information Server (IIS) Version 5.0 aus. Wenn der "Code Red"-Wurm einen Host infiziert, veranlasst er den Host, eine beliebige Reihe von IP-Adressen zu überprüfen und zu infizieren, was zu einem starken Anstieg des Netzwerkverkehrs führt. Dies ist besonders dann problematisch, wenn im Netzwerk redundante Links vorhanden sind und/oder Cisco Express Forwarding (CEF) nicht zum Umschalten von Paketen verwendet wird.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Wie der "Code Red"-Wurm andere Systeme infiziert

Der Wurm "Code Red" versucht, eine Verbindung zu zufällig generierten IP-Adressen herzustellen. Jeder infizierte IIS-Server kann versuchen, denselben Gerätesatz zu infizieren. Sie können die Quell-IP-Adresse und den TCP-Port des Wurms verfolgen, da dieser nicht gesäubert ist. Unicast Reverse Path Forwarding (URPF) kann einen Wurmangriff nicht unterdrücken, da die Quelladresse legal ist.

Advisories, die den "Code Red"-Wurm diskutieren

Diese Ratgeber beschreiben den "Code Red" Wurm und erklären, wie Software, die vom Wurm betroffen ist, gepatcht wird:

- Cisco Security Advisory: "Code Red"-Wurm - Auswirkungen auf Kunden
- Puffer-Overflow für ISAPI-Erweiterungen des Remote IIS-Indexservers
- .ida "Code Red"-Wurm
- CERT? Advisory CA-2001-19 "Code Red" Wurm Exploiting Buffer Overflow in IIS Indexing Service DLL

Symptome

Die folgenden Symptome weisen darauf hin, dass ein Cisco Router vom Wurm "Code Red" betroffen ist:

- Große Anzahl von Datenflüssen in NAT- oder PAT-Tabellen (wenn Sie NAT oder PAT verwenden).
- Große Anzahl von ARP-Anfragen oder ARP-Stürmen im Netzwerk (verursacht durch die IP-Adressprüfung).
- Übermäßige Speichernutzung durch IP-Eingang, ARP-Eingabe, IP-Cache-Speicher und CEF-Prozesse.
- Hohe CPU-Auslastung bei ARP, IP Input, CEF und IPC.
- Hohe CPU-Auslastung auf Unterbrechungsebene bei niedrigen Datenverkehrsraten oder hohe CPU-Auslastung auf Prozessebene bei IP-Eingang, wenn Sie NAT verwenden.

Ein niedriger Speicherzustand oder eine anhaltend hohe CPU-Auslastung (100 Prozent) auf Unterbrechungsebene können dazu führen, dass ein Cisco IOS®-Router neu geladen wird. Das Neuladen wird durch einen Prozess verursacht, der sich aufgrund der Stressbedingungen falsch verhält.

Wenn Sie nicht vermuten, dass Geräte in Ihrer Site vom Wurm "Code Red" infiziert sind oder das Ziel dieses Wurms sind, finden Sie im Abschnitt Zugehörige Informationen weitere URLs, die Ihnen zeigen, wie Sie Probleme beheben können.

Identifizieren des infizierten Geräts

Verwenden Sie Flow Switching, um die Quell-IP-Adresse des betroffenen Geräts zu identifizieren. Konfigurieren Sie den **ip route-cache-Fluss auf allen Schnittstellen, um alle vom Router geswitchten Flüsse aufzuzeichnen.**

Führen Sie nach einigen Minuten den **Befehl show ip cache flow aus, um die aufgezeichneten Einträge anzuzeigen.** In der Anfangsphase der Wurminfektion "Code Red" versucht sich der Wurm zu replizieren. Die Replikation erfolgt, wenn der Wurm HT-Anfragen an beliebige IP-Adressen sendet. Aus diesem Grund müssen Sie nach Cache-Flow-Einträgen mit Zielport 80 (HT, Hex 0050) suchen.

Der **show ip cache flow | include 0050** command display all the cache entries with a TCP port 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
```

Wenn Sie eine ungewöhnlich hohe Anzahl von Einträgen mit derselben Quell-IP-Adresse, der zufälligen Ziel-IP-Adresse[1], DstP = 0050 (HTTP) und Pr = 06 (TCP) finden, haben Sie wahrscheinlich ein infiziertes Gerät gefunden. In diesem Ausgabebeispiel lautet die Quell-IP-Adresse 193.23.45.35 und stammt von VLAN1.

[1]Eine andere Version des Wurms "Code Red", genannt "Code Red II", wählt keine vollständig zufällige Ziel-IP-Adresse. Stattdessen behält "Code Red II" den Netzwerkteil der IP-Adresse bei und wählt einen zufälligen Hostteil der IP-Adresse aus, um weiterzuleiten. Dadurch kann sich der Wurm im selben Netzwerk schneller verbreiten.

"Code Red II" verwendet diese Netzwerke und Masken:

```
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)
```

Ausgeschlossene Ziel-IP-Adressen sind 127.X.X.X und 224.X.X.X, und kein Oktett darf 0 oder 255 sein. Darüber hinaus versucht der Host nicht, sich erneut zu infizieren.

Weitere Informationen finden Sie unter Code Red (II) .

Manchmal können Sie keinen NetFlow ausführen, um einen Infestationsversuch mit "Code Rot" zu erkennen. Dies kann daran liegen, dass Sie eine Codeversion ausführen, die NetFlow nicht unterstützt, oder dass der Router über unzureichenden oder übermäßig fragmentierten Speicher verfügt, um NetFlow zu aktivieren. Cisco empfiehlt, NetFlow nicht zu aktivieren, wenn es mehrere Eingangs-Schnittstellen und nur eine Ausgangsschnittstelle auf dem Router gibt, da die NetFlow-Abrechnung auf dem Eingangspfad durchgeführt wird. In diesem Fall ist es besser, die IP-Abrechnung für die einzige Ausgangsschnittstelle zu aktivieren.

Hinweis: Der **Befehl** ip accounting deaktiviert DCEF. Aktivieren Sie IP Accounting auf keiner Plattform, auf der Sie DCEF-Switching verwenden möchten.

```
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
```

Suchen Sie in der **Befehlsausgabe show ip accounting nach Quelladressen, die versuchen, Pakete an mehrere Zieladressen zu senden.** Wenn sich der infizierte Host in der Scan-Phase befindet, versucht er, HTTP-Verbindungen zu anderen Routern herzustellen. Sie sehen also Versuche, mehrere IP-Adressen zu erreichen. Die meisten dieser Verbindungsversuche schlagen normalerweise fehl. Aus diesem Grund werden nur wenige Pakete übertragen, von denen jedes eine kleine Byteanzahl aufweist. In diesem Beispiel ist es wahrscheinlich, dass 20.1.145.49 und 20.1.104.194 infiziert sind.

Wenn Sie Multi-Layer-Switching (MLS) auf der Catalyst Serie 5000 und der Catalyst Serie 6000 ausführen, müssen Sie verschiedene Schritte unternehmen, um NetFlow Accounting zu aktivieren und den Befall zu erkennen. In einem Cat6000-Switch mit der Supervisor 1 Multilayer Switch Feature Card (MSFC1) oder SUP I/MSFC2 ist NetFlow-basiertes MLS standardmäßig aktiviert, aber der Flow-Modus ist nur Ziel. Daher wird die Quell-IP-Adresse nicht zwischengespeichert. Sie können den Modus "full-flow" aktivieren, um infizierte Hosts mithilfe des **Befehls set mls flow full auf dem Supervisor** nachzuverfolgen.

Verwenden Sie für den Hybrid-Modus den Befehl **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.
```

Verwenden Sie für den nativen IOS-Modus den **Befehl mls flow ip full**:

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

Wenn Sie den Modus "full-flow" aktivieren, wird eine Warnung angezeigt, die auf eine dramatische Zunahme der MLS-Einträge hinweist. Die Auswirkungen der erhöhten MLS-Einträge sind für kurze Zeit zu rechtfertigen, wenn Ihr Netzwerk bereits mit dem "Code Red" Wurm befallen ist. Der Wurm verursacht, dass Ihre MLS-Einträge übertrieben sind und sich im Aufwind befinden.

Um die erfassten Informationen anzuzeigen, verwenden Sie die folgenden Befehle:

Verwenden Sie für den Hybrid-Modus den Befehl **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.
```

Verwenden Sie für den nativen IOS-Modus den Befehl **mls flow ip full**:

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

Wenn Sie den Modus "full-flow" aktivieren, wird eine Warnung angezeigt, die auf eine dramatische Zunahme der MLS-Einträge hinweist. Die Auswirkungen der erhöhten MLS-Einträge sind für kurze Zeit zu rechtfertigen, wenn Ihr Netzwerk bereits mit dem "Code Red" Wurm befallen ist. Der Wurm verursacht, dass Ihre MLS-Einträge übertrieben sind und sich im Aufwind befinden.

Um die erfassten Informationen anzuzeigen, verwenden Sie die folgenden Befehle:

Verwenden Sie für den Hybrid-Modus den **Befehl 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
------------- -------------- ----- ------ ------ ----------------- ---- ----
---- --------- --------- ---------- ----------- -------- --------
```

Hinweis: Alle diese Felder werden ausgefüllt, wenn sie sich im Modus "full-flow" befinden.

Für den nativen IOS-Modus verwenden Sie den Befehl **show mls ip**:

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

Wenn Sie die Quell-IP-Adresse und den Zielport bestimmen, die an dem Angriff beteiligt sind, können Sie MLS auf den Modus "destination-only" (Nur Ziel) zurücksetzen.

Für den Hybrid-Modus verwenden Sie den **Befehl** set mls flow destination:

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

Verwenden Sie für den nativen IOS-Modus den Befehl mls flow **ip destination**:

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

Die Kombination Supervisor (SUP) II/MSFC2 ist vor Angriffen geschützt, da CEF-Switching in der Hardware ausgeführt wird und die NetFlow-Statistiken beibehalten werden. Wenn Sie also den Vollstrom-Modus aktivieren, wird der Router selbst bei einem "Code Red"-Angriff aufgrund des schnelleren Switching-Mechanismus nicht überlastet. Die Befehle zum Aktivieren des Full-Flow-Modus und zum Anzeigen der Statistiken sind auf SUP I/MFSC1 und SUP II/MSFC2 identisch.

Präventionsmethoden

Verwenden Sie die in diesem Abschnitt aufgeführten Techniken, um die Auswirkungen des Wurms "Code Red" auf den Router zu minimieren.

Datenverkehr an Port 80 blockieren

Wenn dies in Ihrem Netzwerk möglich ist, können Sie den "Code Red"-Angriff am einfachsten verhindern, indem Sie den gesamten Datenverkehr zu Port 80 blockieren, dem bekannten Port für WWW. Erstellen Sie eine Zugriffsliste, um IP-Pakete, die für Port 80 bestimmt sind, zu verweigern und diese eingehend auf die Schnittstelle anzuwenden, die der Infektionsquelle gegenübersteht.

Reduzierung der ARP-Eingangsspeicherauslastung

ARP Input verwendet enorme Speicherkapazitäten, wenn eine statische Route auf eine Broadcast-Schnittstelle zeigt. Beispiel:

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

Jedes Paket für die Standardroute wird an das VLAN3 gesendet. Da jedoch keine Next-Hop-IP-Adresse angegeben ist, sendet der Router eine ARP-Anfrage für die Ziel-IP-Adresse. Der nächste Hop-Router für dieses Ziel antwortet mit seiner eigenen MAC-Adresse, es sei denn, Proxy-ARP ist deaktiviert. Die Antwort vom Router erstellt einen zusätzlichen Eintrag in der ARP-Tabelle, in der die Ziel-IP-Adresse des Pakets der Next-Hop-MAC-Adresse zugeordnet ist. Der Wurm "Code Red" sendet Pakete an zufällige IP-Adressen, wodurch ein neuer ARP-Eintrag für jede zufällige Zieladresse hinzugefügt wird. Jeder neue ARP-Eintrag belegt im ARP-Eingabeprozess immer mehr Speicher.

Erstellen Sie keine statische Standardroute zu einer Schnittstelle, insbesondere nicht, wenn die Schnittstelle Broadcast (Ethernet/Fast Ethernet/GE/SMDS) oder Multipoint (Frame Relay/ATM) ist. Jede statische Standardroute muss auf die IP-Adresse des nächsten Hop-Routers zeigen. Nachdem Sie die Standardroute so geändert haben, dass sie auf die nächste Hop-IP-Adresse zeigt, verwenden Sie den Befehl **clear arp-cache**, um alle ARP-Einträge zu löschen. Dieser Befehl behebt das Speicherauslastungsproblem.

Cisco Express Forwarding (CEF) Switching verwenden

Um die CPU-Auslastung eines IOS-Routers zu reduzieren, wechseln Sie von Fast/Optimum/Netflow-Switching zu CEF-Switching. CEF kann durch einige Vorbehalte aktiviert werden. Im nächsten Abschnitt wird der Unterschied zwischen CEF und Fast Switching erläutert. Außerdem werden die Auswirkungen erläutert, die sich aus der Aktivierung von CEF ergeben.

Cisco Express Forwarding und Fast Switching

Aktivieren Sie CEF, um die durch den Wurm "Code Red" verursachte erhöhte Datenverkehrslast zu reduzieren. Die Cisco IOS® Software-Versionen 11.1( )CC, 12.0 und höher unterstützen CEF auf den Cisco 7200/7500/GSR-Plattformen. Unterstützung für CEF auf anderen Plattformen ist in Cisco IOS Software, Version 12.0 oder höher, verfügbar. Sie können das Software Advisor-Tool eingehend nutzen.

Manchmal können Sie CEF aus einem der folgenden Gründe nicht auf allen Routern aktivieren:

- Unzureichender Speicher
- Nicht unterstützte Plattformarchitekturen
- Nicht unterstützte Schnittstellenkapselungen

Fast Switching - Verhalten und Auswirkungen

Das schnelle Switching hat folgende Auswirkungen:

- Datenverkehrsgesteuerter Cache - Der Cache ist leer, bis der Router Pakete wechselt und den Cache füllt.
- Das erste Paket wird prozessgesteuert - das erste Paket wird prozessgesteuert, da der Cache zunächst leer ist.
- Granularer Cache - Der Cache wird mit einer Granularität des spezifischsten RIB-Eintrags (Routing Information Base) in einem Hauptnetz erstellt. Wenn RIB /24s für das Hauptnetz 131.108.0.0 enthält, wird der Cache mit /24s für dieses Hauptnetzwerk erstellt.

- Der /32-Cache wird verwendet -/32-Cache, um die Last für jedes Ziel auszugleichen. Wenn der Cache die Last ausgleicht, wird der Cache mit /32s für dieses Hauptnetz erstellt.**Hinweis:** Diese beiden letzten Probleme können möglicherweise einen riesigen Cache verursachen, der den gesamten Speicher belegt.
- Caching an den wichtigsten Netzwerkgrenzen - Bei der Standardroute erfolgt das Caching an den wichtigsten Netzwerkgrenzen.
- Cache Ager (Cache-Ager): Der Cache-Manager wird jede Minute ausgeführt und überprüft 1/20 (5 Prozent) des Cache auf nicht verwendete Einträge unter normalen Speicherbedingungen und 1/4 (25 Prozent) des Cache in einem niedrigen Speicherzustand (200 KB).

Um die obigen Werte zu ändern, verwenden Sie den Befehl **ip cache-ager-interval X Y Z**, wobei:

- X ist die <0-2147483> Anzahl der Sekunden zwischen ager-Vorgängen. Standardwert = 60 Sekunden.
- Y ist <2-50> 1/(Y+1) Cache bis Alter pro Run (niedriger Arbeitsspeicher). Standard = 4.
- Z ist <3-100> 1/(Z+1) des Cache bis zum Alter pro Lauf (normal). Standardwert = 20.

Dies ist eine Beispielkonfiguration, die **ip cache-ager 60 5 25** verwendet.

```
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
```

Basierend auf der Einstellung Ihres Cache-Senders wird ein bestimmter Prozentsatz Ihrer Cache-Einträge aus der Fast-Cache-Tabelle gelöscht. Wenn Einträge schnell altern, altert ein größerer Anteil der Fast-Cache-Tabellen, und die Cachetabelle wird kleiner. Dadurch verringert sich der Speicherbedarf auf dem Router. Ein Nachteil ist, dass der Datenverkehr für die Einträge, die aus der Cache-Tabelle veraltet wurden, weiterhin fließt. Die anfänglichen Pakete werden prozessgesteuert, was zu einem kurzen Anstieg des CPU-Verbrauchs in der **IP-Eingabe** führt, bis ein neuer Cache-Eintrag für den Datenfluss erstellt wird.

Aus den Cisco IOS Software-Versionen 10.3(8), 11.0(3) und höher wird der IP-Cache-Manager anders behandelt, wie hier erläutert:

- Die Befehle **ip cache-ager interval** und **ip cache-invalidate-delay** sind nur verfügbar, wenn der **interne** Service-Befehl in der Konfiguration definiert ist.
- Wenn der Zeitraum zwischen dem Ausführen der ager-Invalidierung auf 0 festgelegt ist, wird der ager-Prozess vollständig deaktiviert.
- Zeit wird in Sekunden ausgedrückt.

Hinweis: Wenn Sie diese Befehle ausführen, nimmt die CPU-Auslastung des Routers zu. Verwenden Sie diese Befehle nur, wenn es unbedingt erforderlich ist.

```
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
```

Vorteile von CEF

- Die FIB-Tabelle (Forwarding Information Base) basiert auf der Routing-Tabelle. Daher existieren Weiterleitungsinformationen, bevor das erste Paket weitergeleitet wird. Die FIB enthält auch /32-Einträge für direkt verbundene LAN-Hosts.
- Die ADJ-Tabelle (Adjacency) enthält die Layer-2-Umschreibinformationen für Next-Hops und direkt verbundene Hosts (ein ARP-Eintrag erstellt eine CEF-Adjacency).
- Mit CEF gibt es kein Cache-Manager-Konzept, um die CPU-Auslastung zu steigern. Ein FIB-Eintrag wird gelöscht, wenn ein Eintrag in einer Routing-Tabelle gelöscht wird.

Achtung: Eine Standardroute, die auf eine Broadcast- oder Multipoint-Schnittstelle zeigt, bedeutet, dass der Router ARP-Anfragen für jedes neue Ziel sendet. ARP-Anforderungen des Routers können eine riesige Adjacency-Tabelle erstellen, bis dem Router der Arbeitsspeicher ausgeht. Wenn CEF den Speicher nicht reserviert, deaktiviert sich CEF/DCEF selbst. Sie müssen CEF/DCEF erneut manuell aktivieren.

Beispiel für das Ergebnis: CEF

Hier sehen Sie einige Beispielausgabe des **Befehls show ip cef summary, der die Speichernutzung anzeigt.** Diese Ausgabe ist ein Snapshot eines Cisco 7200-Routenservers mit Cisco IOS Software Release 12.0.

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

Adjacency Table has 16 adjacencies


Router>show processes memory | include CEF
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
```

```
  73   0     147300       1700     146708          0          0 CEF process
  84   0        608          0       7404          0          0 CEF Scanner
```

```
Router>show processes memory | include BGP

   2   0    6891444    6891444       6864          0          0 BGP Open
  80   0       3444       2296       8028          0          0 BGP Open
  86   0     477568     476420       7944          0          0 BGP Open
  87   0 2969013892  102734200  338145696          0          0 BGP Router
  88   0   56693560 2517286276       7440     131160    4954624 BGP I/O
  89   0      69280   68633812      75308          0          0 BGP Scanner
  91   0    6564264    6564264       6876          0          0 BGP Open
 101   0    7635944    7633052       6796        780          0 BGP Open
 104   0    7591724    7591724       6796          0          0 BGP Open
 105   0    7269732    7266840       6796        780          0 BGP Open
 109   0    7600908    7600908       6796          0          0 BGP Open
 110   0    7268584    7265692       6796        780          0 BGP Open
```

```
Router>show memory summary | include FIB

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

```
Router>show memory summary | include CEF

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

```
Router>show memory summary | include adj

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

Wichtige Überlegungen

Wenn die Anzahl der Datenflüsse groß ist, benötigt CEF in der Regel weniger Arbeitsspeicher als schnelles Switching. Wenn der Speicher bereits durch einen schnellen Switching-Cache belegt ist, müssen Sie den ARP-Cache (durch den Befehl **clear ip arp**) löschen, bevor Sie CEF aktivieren.

Hinweis: Wenn Sie den Cache löschen, wird eine Spitze in der CPU-Auslastung des Routers verursacht.

"Code Red" - Häufig gestellte Fragen und deren Antworten

F. Ich verwende NAT und erlebe eine CPU-Auslastung von 100 Prozent bei IP Input. Wenn ich show proc cpu ausführe, ist meine CPU-Auslastung hoch im Interrupt-Level - 100/99 oder 99/98. Kann dies mit "Code Red" in Zusammenhang stehen?

Antwort: Es wurde kürzlich ein NAT Cisco Bug (CSCdu63623 (nur registrierte Kunden) behoben, der Skalierbarkeit beinhaltet. Bei zehntausenden NAT-Datenflüssen (je nach Plattformtyp) verursacht der Fehler eine CPU-Auslastung von 100 Prozent auf Prozess- oder Unterbrechungsebene.

Um festzustellen, ob dieser Fehler der Grund ist, führen Sie den Befehl **show align** aus, und überprüfen Sie, ob auf dem Router Ausrichtungsfehler auftreten. Wenn Alignment-Fehler oder fehlerhafte Speicherzugriffe angezeigt werden, führen Sie den Befehl **show align (**Ausrichten **anzeigen**) mehrmals aus, und überprüfen Sie, ob die Fehler auftreten. Wenn die Anzahl der Fehler zunimmt, können Alignment-Fehler die Ursache für eine hohe CPU-Auslastung auf Unterbrechungsebene sein, nicht aber für Cisco Bug CSCdu63623 (nur registrierte Kunden). Weitere Informationen finden Sie unter Fehlerbehebung bei Fehlern bei Funkstörungen und Alignment.

Der Befehl **show ip nat translation** zeigt die Anzahl der aktiven Übersetzungen an. Der Kernpunkt für einen NPE-300-Prozessor liegt bei etwa 20.000 bis 40.000 Übersetzungen. Diese Zahl variiert je nach Plattform.

Dieses Kernschmelzen-Problem wurde zuvor von einigen Kunden beobachtet, aber nach "Code Red" haben mehr Kunden dieses Problem. Die einzige Lösung besteht darin, NAT (anstelle von PAT) auszuführen, sodass weniger aktive Übersetzungen vorhanden sind. Wenn Sie einen 7200 haben, verwenden Sie ein NSE-1, und senken Sie die NAT-Timeout-Werte.

F. Ich führe IRB aus und im HyBridge-Eingabeprozess kommt es zu einer hohen CPU-Auslastung. Warum geschieht das? Bezieht sich dies auf "Code Red"?

Antwort: Der HyBridge-Eingabeprozess verarbeitet alle Pakete, die nicht durch den IRB-Prozess schnell umgeschaltet werden können. Der IRB-Prozess kann ein Paket nicht schnell umschalten. Dies kann folgende Gründe haben:

- Das Paket ist ein Broadcast-Paket.
- Das Paket ist ein Multicast-Paket.
- Das Ziel ist unbekannt, und ARP muss ausgelöst werden.
- Es gibt Spanning Tree BPDUs.

Bei HyBridge-Eingang treten Probleme auf, wenn sich in derselben Bridge-Gruppe Tausende Point-to-Point-Schnittstellen befinden. Bei HyBridge Input treten auch Probleme auf (jedoch in

geringerem Maße), wenn sich in derselben Multipoint-Schnittstelle Tausende VSs befinden.

Was sind mögliche Gründe für Probleme mit IRB? Angenommen, ein mit "Code rot" infiziertes Gerät prüft IP-Adressen.

- Der Router muss eine ARP-Anfrage für jede Ziel-IP-Adresse senden. Eine Flut von ARP-Anfragen resultiert für jede VC in der Bridge-Gruppe für jede gescannte Adresse. Der normale ARP-Prozess verursacht kein CPU-Problem. Wenn jedoch ein ARP-Eintrag ohne Bridge-Eintrag vorhanden ist, überflutet der Router Pakete, die für Adressen bestimmt sind, für die bereits ARP-Einträge vorhanden sind. Dies kann zu einer hohen CPU-Auslastung führen, da der Datenverkehr prozessgesteuert weitergeleitet wird. Um das Problem zu vermeiden, erhöhen Sie die Überbrückungs-Aging-Zeit (Standardeinstellung: 300 Sekunden oder 5 Minuten), um das ARP-Timeout (Standardeinstellung: 4 Stunden) abzugleichen oder zu überschreiten, sodass die beiden Timer synchronisiert werden.
- Die Adresse, die der Endhost zu infizieren versucht, ist eine Broadcast-Adresse. Der Router erfüllt die Entsprechung einer Subnetzübertragung, die vom HyBridge-Eingabeprozess repliziert werden muss. Dies ist nicht der Fall, wenn der Befehl **no ip directed-broadcast** konfiguriert wurde. In Cisco IOS Software Release 12.0 ist der Befehl **ip directed-broadcast** standardmäßig deaktiviert, wodurch alle IP-gesteuerten Broadcasts verworfen werden.
- Im Folgenden finden Sie einen Seitenhinweis, der nicht mit "Code Red" in Zusammenhang steht und sich auf IRB-Architekturen bezieht:Layer-2-Multicast- und Broadcast-Pakete müssen repliziert werden. Aus diesem Grund kann ein Problem mit IPX-Servern, die auf einem Broadcast-Segment ausgeführt werden, die Verbindung herabsetzen. Sie können Teilnehmerrichtlinien verwenden, um das Problem zu vermeiden. Weitere Informationen finden Sie unter x Digital Subscriber Line (xDSL) Bridge Support. Sie müssen auch Bridge-Zugriffslisten in Betracht ziehen, die die Art des Datenverkehrs einschränken, der durch den Router geleitet werden darf.
- Um dieses IRB-Problem zu beheben, können Sie mehrere Bridge-Gruppen verwenden und sicherstellen, dass eine Eins-zu-Eins-Zuordnung für BVIs, Subschnittstellen und VCs vorhanden ist.
- RBE ist IRB überlegen, da es den Bridging-Stack komplett vermeidet. Sie können von IRB zu RBE migrieren. Diese Fehler von Cisco fördern eine solche Migration:CSCdr1146 (nur registrierte Kunden)CSCdp18572 (nur registrierte Kunden)CSCds40806 (nur registrierte Kunden)

Q.Meine CPU-Auslastung ist auf Interrupt-Ebene hoch, und ich erhalte beim Testen eines Anzeigeprotokolls Pinsel. Die Datenverkehrsrate ist ebenfalls nur etwas höher als normal. Was ist der Grund dafür?

Antwort: Hier ein Beispiel für die Ausgabe des Befehls **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
```

Überprüfen Sie, ob Sie sich bei der Konsole anmelden. Wenn ja, prüfen Sie, ob HTTP-Datenverkehrsanforderungen vorliegen. Überprüfen Sie anschließend, ob Zugriffslisten mit

Protokollschlüsselwörtern oder Debuggen vorhanden sind, die bestimmte IP-Flüsse überwachen. Wenn es immer mehr Flushes gibt, kann dies daran liegen, dass die Konsole, normalerweise ein 9600-Baud-Gerät, die Menge der empfangenen Informationen nicht verarbeiten kann. In diesem Szenario deaktiviert der Router Interrupts und verarbeitet lediglich Konsolenmeldungen. Die Lösung besteht darin, die Konsolenprotokollierung zu deaktivieren oder alle von Ihnen ausgeführten Protokolltypen zu entfernen.

F. Ich kann zahlreiche HTTP-Verbindungsversuche auf meinem IOS-Router sehen, auf dem ein IP-HTTP-Server ausgeführt wird. Ist das auf den "Code Red" Wurmscan zurückzuführen?

A. "Code Red" kann hier der Grund sein. Cisco empfiehlt, den Befehl **ip http server** auf dem IOS-Router zu deaktivieren, damit er nicht mit zahlreichen Verbindungsversuchen infizierter Hosts umgehen muss.

Workarounds

Es gibt verschiedene Workarounds, die in den Advisories diskutiert werden, die den Abschnitt "Code Red" Wurm behandeln. Informationen zu den Problemumgehungen finden Sie in den Ratgebern.

Eine andere Methode zum Blockieren des "Code Red"-Wurms an den Netzwerkeingangspunkten verwendet Network-Based Application Recognition (NBAR) und Access Control Lists (ACLs) in der IOS-Software auf Cisco Routern. Verwenden Sie diese Methode in Verbindung mit den empfohlenen Patches für IIS-Server von Microsoft. Weitere Informationen zu dieser Methode finden Sie unter Verwenden von NBAR und ACLs zum Blockieren des "Code Red"-Wurms an den Netzwerk-Eingangspunkten.

Zugehörige Informationen

- Fehlerbehebung bei Speicherfehlern
- Fehlerbehebung: Pufferlecks
- Fehlerbehebung bei hoher CPU-Auslastung auf Cisco Routern
- Fehlerbehebung bei Router-Abstürzen
- Fehlerbehebung bei TechNotes - Router
- Fehlerbehebung beim Router
- Technischer Support und Dokumentation für Cisco Systeme