处理起因于" Code Red "蠕虫的mallocfail和高CPU利用率

Contents

Introduction

本文描述" Code Red "蠕虫，并且蠕虫能的Cisco路由环境引起的问题。本文也描述技术防止蠕虫的袭击并且提供描述相关问题的解决方案的相关建议的链路。

"Code Red "蠕虫利用微软互联网Information塞尔韦尔(IIS)版本5.0的索引服务的一个弱点。当" Code Red "蠕虫感染主机时，造成主机探查和传染IP地址一系列随机的，导致在网络流量的猛增。

这是特别有问题的，如果有在网络的冗余链路并且/或者思科快速转发(CEF)没有用于转换信息包。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

" Code Red "蠕虫如何传染其他系统

"Code Red "蠕虫尝试连接到随机地生成的IP地址。每个被传染的IIS服务器能尝试传染同一个一套设备。因为没有被伪装，您能跟踪蠕虫的IP原地址和TCP端口。因为源地址是合法的，单播逆向路径转发(URPF)不能抑制蠕虫攻击。

讨论" Code Red "蠕虫的建议

这些建议描述" Code Red "蠕虫，并且解释如何修补蠕虫的影响的软件：

- **Cisco安全建议:**" Code Red "蠕虫-用户影响
- 远程IIS索引服务器ISAPI扩展缓冲区溢出
- .ida " Code Red "蠕虫
- CERT ？利用在IIS索引服务DLL的资询CA-2001-19 " Code Red "蠕虫缓冲区溢出

症状

这是指示的一些症状Cisco路由器是受" Code Red "蠕虫的影响的：

- 流的大量在NAT或PAT表里(如果使用NAT或PAT)。
- ARP请求或ARP风暴的大量在网络(造成由IP地址扫描)。
- 由IP输入、ARP输入、IP缓存老化器和CEF进程的额外的内存使用。
- 在ARP， IP输入、CEF和IPC的高CPU利用率。
- 在中断级别的高CPU利用率以低业务量费率或者在流程级的高CPU利用率在IP输入，如果使用NAT。

低内存状况或持续的高CPU利用率(100%)在中断级别能造成Cisco IOS路由器重新载入。重新加载

是由行为不端由于重点条件的进程引起的。

如果不怀疑设备在您的站点传染由或是" Code Red "蠕虫的目标，请参阅相关信息部分关于关于怎样的另外的URL排除您遇到的所有问题故障。

识别感染的设备

请使用流交换识别受影响的设备的IP原地址。配置在所有接口的ip route-cache flow记录路由器交换的所有流。

在几分钟之后，请发出show ip cache flow命令查看记录条目。在" Code Red "蠕虫传染的初期阶段期间，蠕虫设法复制自己。当蠕虫发送HT请求到随机的IP地址，复制发生。所以，您必须寻找与目的地端口80 (HT的缓存流条目。 ， 0050在十六进制)。

show ip cache flow|包括命令显示与TCP端口80的所有缓存条目的**0050** (0050在十六进制) ：

```
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
```

如果看到条目的异常地大数字用同样IP原地址、随机目的地IP地址[1]， DstP = 0050 (HTTP)和PR = 06 (TCP)，您很可能找出一个感染的设备。在此输出示例中， IP原地址是193.23.45.35并且来自VLAN1。

1Another " Code Red "蠕虫的版本，称为“红色代码II”，不选择一个完全随意的目的地IP地址。反而，“红色代码II”保持IP地址的网络部分，并且选择IP地址的一个随机的主机部分为了传播。这允许蠕虫在同一网络内快速地传播自己。

“红色代码II”使用这些网络和掩码：

```
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)
```

被屏蔽的目标IP地址是127.X.X.X和224.X.X.X和没有八位位组准许是0或255。另外，主机不尝试再传染自己。

欲知更多信息，请参见红色代码(ii) 。

有时，您不能运行Netflow发现" Code Red "袭击尝试。这可以是因为您运行不支持Netflow的编码版本，或者，因为路由器有不足或非常地被分段的内存对以启用NetFlow。Cisco建议您不以启用NetFlow，当只有多个入口接口和一个输出接口在路由器时，因为NetFlow记账在入口路径执行。在

这种情况下，是好对在孤立输出接口的enable (event) IP记帐。

Note: ip accounting命令功能失效DCEF。不在您要使用DCEF交换的任何平台的enable (event) IP记帐。

```
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
```

在show ip accounting命令输出中，请寻找尝试发送信息包到多个目的地地址的源地址。如果感染的主机是在扫描阶段，尝试建立与其他路由器的HTTP连接。因此您将看到尝试到达多个IP地址。大多数正常这些连接尝试失败。所以，您看到仅很小数量的信息包传输，其中每一与小的字节数。在本例中，很可能20.1.145.49和20.1.104.194被传染。

当您运行在Catalyst 5000 Series和Catalyst 6000 Series时的多层交换(MLS)，您必须采取不同的步骤到认为的以启用NetFlow和搜寻袭击。在Cat6000交换机中配备有Supervisor 1多层交换特性卡(MSFC1)默认情况下或SUP I/MSFC2，基于网络数据流的MLS被启用，但是流模式目的地专用。所以，没有缓存IP原地址。您能跟踪感染的主机的enable (event) “全流的”模式在set mls flow full命令帮助下在Supervisor。

对于混合模式，请使用**set mls flow full命令**：

```
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.
```

对于本地IOS模式，请使用mls flow ip full命令：

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

当您enable (event) “全流的”模式，警告显示指示在MLS交换项的一个显著增长。如果您的网络已经骚扰" Code Red "蠕虫，增加的MLS交换项的影响是情有可原的在短时长。蠕虫造成您的MLS交换项额外和上涨。

要查看收集的信息，请使用这些命令：

对于混合模式，请使用**set mls flow full命令**：

```
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.
```

对于本地IOS模式，请使用**mls flow ip full命令**：

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

当您enable (event) “全流的”模式，警告显示指示在MLS交换项的一个显著增长。如果您的网络已经骚扰" Code Red "蠕虫，增加的MLS交换项的影响是情有可原的在短时长。蠕虫造成您的MLS交换项额外和上涨。

要查看收集的信息，请使用这些命令：

对于混合模式，请使用**show mls ent命令**：

```
6500-sup(enable)show mls ent
Destination-IP  Source-IP     Prot  DstPrt SrcPrt Destination-Mac   Vlan EDst
ESrc DPort     SPort     Stat-Pkts  Stat-Bytes  Uptime   Age
--------------- --------------- ----- ------ ------ ----------------- ---- ----
---- --------- --------- ---------- ----------- -------- --------
```

Note: 当他们在“全流的”模式下时，所有这些字段填写。

对于本地IOS模式，请使用**show mls ip命令**：

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

当您确定在攻击时和目的地端口涉及的IP原地址，您能送回MLS到“目的地专用”模式。

对于混合模式请使用**set mls flow destination命令**：

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

对于本地IOS模式，请使用**mls flow ip destination命令**：

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

Supervisor (Sup) II/MSFC2组合保护免受攻击，因为CEF交换在硬件里被执行，并且Netflow统计数据被维护。因此，即使在一次" Code Red "攻击期间，如果enable (event)全流模式，路由器没有陷入沼泽，由于快的交换机制。对enable (event)全流模式的命令和显示统计数据是相同的在SUP I/MFSC1和SUP II/MSFC2。

预防技术

请使用列出的技术在此部分使" Code Red "蠕虫减到最小的影响对路由器。

阻塞数据流对端口80

如果它是可行的在您的网络，防止" Code Red "攻击的简便的方法是阻塞所有数据流对端口80，是WWW的众所周知的端口。创建访问列表丢弃IP信息包被注定对端口80和应用它入站在面对传染来源的接口。

减少ARP输入内存用量

ARP输入用完巨大的内存数量，当对一个广播接口的静态路由点，象这样：

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

默认路由的每个信息包被发送到VLAN3。然而，没有指定的下一跳IP地址，然后路由器发送目的地IP地址的一个ARP请求。除非代理ARP是失效的，该目的地的下一跳路由器回复以其自己的MAC地址。从路由器的回复在信息包的目的地IP地址被映射对下一跳MAC地址的ARP表里创建其它条目。" Code Red "蠕虫发送信息包到随机的IP地址，添加每随机目的地目标地址的新的ARP条目。每新的ARP条目浪费越来越多的内存在ARP输入进程下。

请勿创建静态默认路由对接口，特别是如果接口广播(以太网/快速地Ethernet/GE/SMDS)或多点(帧Relay/ATM)。所有静态默认路由必须指向下一跳路由器的IP地址。在您更改默认路由指向下一跳IP地址后，请使用**clear arp-cache命令**清除所有ARP条目。此命令解决内存利用率问题。

请使用思科快速转发

为了降低在IOS路由器的CPU利用率，从快速地/最佳/Netflow交换请变成CEF交换。有一些个警告对enable (event) CEF。下个部分讨论在CEF和快速的交换之间的区别，并且说明暗示，当您enable (event) CEF。

Cisco快速转发与快速的交换

缓和增加的数据流负载的Enable (event) CEF引起由" Code Red "蠕虫。Cisco IOS软件版本11.1 () CC， 12.0，及以后支持CEF在Cisco 7200/7500/GSR平台。CEF的技术支持在其他平台是可用的在Cisco IOS Software Release 12.0或以上。您能用软件建议工具进一步调查。

有时，您不能在所有路由器的enable (event) CEF由于这些原因之一：

- 内存不足
- 不支持的平台体系结构
- 不支持的接口封装

快速的交换行为和暗示

这是暗示，当您使用快速的交换时：

- 数据流被驱动的高速缓冲存储器—高速缓冲存储器是空的直到路由器交换机信息包并且填充高速缓冲存储器。
- 第一个信息包是被交换的进程—，因为高速缓冲存储器是最初空的，第一个信息包被过程交换。

- 粒状高速缓冲存储器—高速缓冲存储器被建立在一个主网的最特定的路由信息库(RIB)条目零件的粒度。如果RIB有主网的131.108.0.0 /24s，高速缓冲存储器用此主要网络的/24s建立。
- 使用/32高速缓冲存储器— /32高速缓冲存储器用于均衡每个目的地的负荷。当高速缓冲存储器均衡负荷时，高速缓冲存储器用该主网的/32s建立。**Note:** 这些前两个问题能潜在导致将浪费所有内存的一个巨大的高速缓冲存储器。
- 在主要网络边界的缓存—使用默认路由，缓存进行在主要网络边界。
- 缓存老化器—缓存老化器每分钟运行并且检查1/20th (5%)高速缓冲存储器未使用项在正常存储器状况下和1/4 (25%)在一个低内存状况(200k)的高速缓冲存储器。

为了更改上述值，请使用**ip cache-ager-interval X Y Z命令**，其中：

- x是秒钟的<0-2147483>编号在老化运行之间的。默认值= 60秒。
- Y是<2-50>更新的高速缓冲存储器1/(Y+1)每运行(低内存)。默认值= 4。
- Z是<3-100>更新的高速缓冲存储器1/(Z+1)每运行(正常)。默认值= 20。

这是使用**ip cache-ager 60 5 25的**配置示例。

```
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
```

基于您的缓存老化器设置，您的缓存条目使用周期的某百分比在您快速的缓存表外面。当快速条目使用周期，快速的缓存表的大部分更新时和缓存表变得更小。结果，在路由器的内存消耗量减少。缺点是数据流继续为更新在缓存表外面的条目流。初始信息包被过程交换的在**被输入的IP的**CPU消耗导致一次短的阻止，直到新的缓存条目为流被建立。

从Cisco IOS Software Releases 10.3(8)， 11 .0 (3)及以后， IP缓存老化器不同处理，按照说明这里：

- 只有当**service internal命令**在配置，被定义**ip cache-ager-interval**和**ip cache-invalidate-delay**命令是可用的。
- 如果在老化无效运行之间的周期设置到0，老化进程完全地被禁用。
- 时间以秒钟表示。

Note: 当您执行这些命令时，路由器的CPU利用率增加。请使用这些命令，只有当绝对必要。

```
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
```

CEF的优点

- 转发信息库(FIB)表根据路由表被构件。所以，在转发前，转发信息存在第一个信息包。FIB也包含直接地被连接的LAN主机的/32条目。
- 邻接(ADJ)表包含下个跳跃和直接连接的主机的(ARP条目第2层重写信息创建CEF邻接)。
- 没有与阻止CPU利用率的CEF的缓存老化器概念。如果路由表条目被删除， FIB条目被删除。

警告： 再次，指向广播或多点接口的默认路由意味着路由器发送每新建目标的ARP请求。从路由器的ARP请求潜在创建一个巨大的邻接表，直到路由器用尽内存。如果CEF不能分配内存CEF/DCEF禁用自己。您将手工需要enable (event) CEF/DCEF再。

输出示例: ：CEF

这是若干输出示例: show ip cef summary命令，那显示存储器使用。此输出是从Cisco7200路由服务器的一个快照有Cisco IOS Software Release 12.0的。

```
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
```

要考虑的事

当流的数量大时，CEF比快速地交换典型地浪费较少内存。如果内存由一快速的交换缓存已经浪费，您必须清除ARP高速缓存(通过**clear ip arp命令**)，在您enable (event) CEF前。

Note: 当您清除高速缓冲存储器时，阻止的路由器的CPU利用率导致。

" Code Red "常见问题和他们的答案

Q. 我使用NAT，并且体验100在IP输入的CPU利用率百分比利用率。当我执行show proc cpu时，我的CPU利用率是高在中断级别- 100/99或99/98。这能否与" Code Red "有关？

A.那里最近被修正介入可扩展性的NAT Cisco Bug (CSCdu63623 (仅限注册用户))。当有数万NAT流(根据平台类型)，Bug导致100 CPU利用率百分比利用率在进程或中断级别。

为了确定此Bug是否是原因，请发出**show align命令**，并且验证路由器是否面对校正错误。如果看到校正错误或欺骗性内存访问，请发出**show align命令**两三次并且检查错误是否上涨。如果错误的数量上涨，校正错误可以是高CPU利用率的原因在中断级别，而不是Cisco Bug CSCdu63623 (仅限注册用户)。欲知更多信息，请参见排除欺骗访问和校正错误故障。

show ip nat translation命令显示有效转换的数量。NPE-300组处理器的熔毁点是大约20,000个到40,000个转换。此编号变化基于平台。

此熔毁问题由两三位用户以前观察，但是在" Code Red "以后，更多用户遇到了此问题。唯一的解决方法是运行NAT (而不是PAT)，因此有少量有效转换。如果有一7200，请使用一NSE-1，并且降低NAT超时值。

Q. 我在hybrIDge输入流程中运行IRB，并且遇到高CPU利用率。为什么会发生这种情况？它是否是和有关系" Code Red " ？

A.hybrIDge输入流程处理不可能由IRB进程快速交换的所有信息包。快速交换信息包的IRB进程的无法可以是，由于：

- 信息包是广播包。
- 信息包是组播信息包。
- 目的地是未知和ARP需要被触发。
- 有生成树BPDU。

如果有千位点到点接口在同一个网桥组中， Hybridge输入遇到问题。Hybridge输入也遇到问题(但是较小程度)，如果有千位在同一个多点接口的VSs。

什么是问题的可能的来源的IRB ？假设，设备感染" Code Red "扫描IP地址。

- 路由器需要发送每个目的地IP地址的一个ARP请求。一群ARP请求在每个VC在网桥组中结果被扫描的每个地址的。正常ARP进程不引起一个CPU问题。然而，如果没有网桥条目，有ARP条目，为ARP条目已经存在的地址注定了的路由器泛滥的信息包。因为数据流进程交换，这能引起高CPU利用率。避免问题，增加过期时间(默认值300秒或5分钟)匹配或超出ARP超时(默认值4小时)，以便脚踏两条船者同步。
- 终端主机尝试传染的地址是广播地址。路由器执行需要由hybrIDge输入流程复制子网广播的等同。如果配置，这不发生**no ip directed-broadcast命令**。默认情况下从Cisco IOS Software Release 12.0， **ip directed-broadcast命令**被禁用，造成所有IP处理的广播下降。
- 这是旁注，无关与" Code Red "和相关对IRB体系结构：第2层组播和广播包需要被复制。所以，在广播分段运行的IPX服务器的一个问题能减少链路。您能使用用户策略避免问题。欲知更多信息，请参见x数字用户线路(xDSL)网桥支持。您必须也考虑网桥访问列表，限制允许的流量类型穿过路由器。
- 为了缓和此IRB问题，您能使用广泛网桥组，并且保证有BVI、sub-interface和VC的一对一映射。
- 因为一共，避免桥接堆栈RBE在IRB是优越。您能移植到从IRB的RBE。这些Cisco Bug启发这样迁移：CSCdr11146 (仅限注册用户)CSCdp18572 (仅限注册用户)CSCds40806 (仅限注册用户)

Q.My CPU利用率是高在中断级别，并且我接受冲洗，如果我尝试show log。流量速率高于正常也只有些。什么是对此的原因？

A.这是**show logging命令**输出的示例：

```
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
```

证实您是否记录到控制台。如果那样，请证实是否有数据流HTTP请求。其次，检查是否有观看特定IP与日志关键字的任何访问列表或调试流。如果冲洗上涨，可以这是因为控制台，通常一个9600波特设备，无法处理接收的信息量。在此方案中，路由器功能失效中断，并且处理控制台信息。解决方案将禁用控制台记录或取消记录您的任何类型请执行。

Q. 我能看到在运行ip http server的我的IOS路由器的许多HTTP连接尝试。这是否是由于" Code Red "蠕虫扫描？

A. " Code Red "可以原因在这里。Cisco建议您禁用**ip http server命令**在IOS路由器，以便不需要处理从感染的主机的许多连接尝试。

解决方法

有在建议讨论讨论" Code Red "蠕虫部分的多种解决方法。请参见解决方法的建议。

阻拦" Code Red "蠕虫的另一个方法在网络入口点使用基于网络应用的识别(NBAR)和访问控制列表(ACL)在IOS软件内在Cisco路由器。与推荐的补丁一道请使用此方法从Microsoft的IIS服务器。关于此方法的更多信息，请参见使用NBAR和ACL阻拦" Code Red "蠕虫在网络入口点。

Related Information

- 排除存储器问题故障
- 排除缓冲泄漏故障
- 对 Cisco 路由器上的 CPU 使用率过高进行故障排除
- 路由器崩溃故障排除
- 排除TechNotes故障-路由器
- 排除路由器故障
- Technical Support & Documentation - Cisco Systems