# 如何解决“红色代码”蠕虫引起的 mallocfail 和 CPU 使用率过高的问题

## 目录



## 简介

本文描述″ Code Red ″蠕虫病毒，并且蠕虫病毒能的思科路由环境引起的问题。本文也描述技术防止蠕虫病毒的袭击并且提供链路给描述相关问题的解决方案的相关建议。

“Code Red”蠕虫造成Microsoft Internet Information Server(IIS)版本5.0索引服务容易遭到攻击的弱点。当″ Code Red ″蠕虫病毒感染主机时，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)没有用于转换数据包。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

## ″ Code Red ″蠕虫病毒如何传染其他系统

″″″Code Red″″蠕虫试图连接到随机生成的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，您能跟踪蠕虫病毒的源IP地址和TCP端口。因为源地址法律，单播逆向路径转发(URPF)不能抑制蠕虫病毒攻击。

## 有关“红色代码”蠕虫的建议

这些建议描述″ Code Red ″蠕虫病毒，并且解释如何修补蠕虫病毒的影响的软件：

- Cisco安全建议:″ Code Red ″蠕虫病毒-客户影响
- 远程IIS索引服务器网络服务器ISAPI扩展缓冲区溢出
- .ida ″ Code Red ″蠕虫病毒
- CERT ？利用在IIS索引服务DLL的资询CA-2001-19 ″ Code Red ″蠕虫病毒缓冲区溢出

## 症状

这是指示的一些症状Cisco路由器是受″ Code Red ″蠕虫病毒的影响的：

- 流大量在NAT的或PAT表(如果使用NAT或PAT)。
- ARP请求或ARP风暴大量在网络(造成由IP地址扫描)。
- IP输入、ARP输入、IP Cache Ager和CEF处理过程使用过多内存。
- ARP、IP输入、CEF和IPC中CPU利用率过高。
- 在中断级别的在进程层面的高CPU利用率以低业务量速率或者高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(100百分比)在中断级别能造成Cisco IOSÃ¯Â¿Â½路由器重新加载。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 ″蠕虫病毒的目标，请参阅相关信息部分关于关于怎样的另外的URL排除故障您遇到的所有问题。

## 识别感染的设备

请使用流交换识别受影响的设备的源IP地址。在所有接口上配置ip route-cache flow，记录路由器交换的所有数据流。

在几分钟之后，请发出show ip cache flow命令查看已录制条目。在″ Code Red ″蠕虫病毒传染的初期阶段期间，蠕虫病毒设法复制。当蠕虫病毒发送HT请求对随机的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
```

如果异常地看到条目一大量用同样源IP地址、随机目的地IP地址1、DstP = 0050 (HTTP)和PR = 06 (TCP)，您很可能查找感染的设备。在本例中输出示例，源IP地址是193.23.45.35并且来自VLAN1。

lAnother ″ Code Red ″蠕虫病毒的版本，呼叫“红色代码II”，不选择一完全随意的目的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。通过这种方式，它可以在同一网络范围内更快地传播。

“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和没有八位位组允许是0或255。另外，主机不尝试再传染自己。

欲知更多信息，参考红色代码(ii) 。

有时，您不能运行Netflow检测" 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。思科建议您不以启用NetFlow，当只有多入口接口和一出口接口在路由器时，因为NetFlow记账在入口路径执行。在这种情况下，最好在独立的出口接口上启用IP记帐功能。

注意： ip accounting命令功能失效DCEF。请勿启用在您要使用DCEF交换的任何平台的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，请寻找尝试发送数据包到多个目的地地址的源地址。如果感染的主机是在扫描相位，尝试建立对其他路由器的HTTP连接。因此您将看到尝试到达多个IP地址。多数这些正常连接尝试失败。所以，您看到仅很小数量的数据包转接，其中每一与小字节数。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系列和Catalyst 6000系列时的多层交换(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启用，但是流模式目的地专用。所以，没有缓存源IP地址。您能启动“全流的”模式在set mls flow full命令帮助下搜寻感染的主机在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
```

当您启动“全流的”模式时，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 "蠕虫病毒，增加的MLS交换项的影响是情有可原的在短时长。蠕虫病毒造成您的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
```

当您启动“全流的”模式时，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 "蠕虫病毒，增加的MLS交换项的影响是情有可原的在短时长。蠕虫病毒造成您的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
--------------- --------------- ----- ------ ------ ----------------- ---- ----
---- --------- --------- ---------- ----------- -------- --------
```

注意： 当他们在“全流的”模式时，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源IP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组合从攻击保护，因为CEF交换在硬件里被执行，并且Netflow统计信息被维护。因此，即使在" Code Red "攻击期间，如果启动全流模式，路由器没有陷入沼泽，由于快的交换机制。命令启动全流模式和显示统计信息是相同的在SUP I/MFSC1和SUP II/MSFC2。

# 预防技术

请使用列出的技术在此部分最小化" Code Red "蠕虫病毒的影响在路由器。

## 阻塞流量给波尔特80

如果它是可行在您的网络，防止" Code Red "攻击的简便的方法是阻塞所有流量对端口80，是WWW的公认端口。构件access-list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输入用完大量内存，当对一个广播接口的静态路由点，象这样：

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

默认路由的每数据包发送对VLAN3。然而，没有指定的下一跳IP地址，然后路由器发送目的IP地址的一个ARP请求。该目的地回复的下一跳路由器与其自己的MAC地址，除非代理ARP禁用。从路由器的回复在数据包目的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 "蠕虫病毒发送数据包对随机的IP地址，添加每随机目的地目标地址的新的ARP条目。其中每一新建的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Ethernet/GE/SMDS)或多点(帧中继/ATM)。所有静态默认路由必须指向下一跳路由器的IP地址。在您更改了指向下一跳IP地址的默认路由之后，请使用clear arp-cache命令，以清除所有ARP条目。此命令解决存储器利用率问题。

## 请使用思科快速转发

为了降低在IOS路由器的CPU利用率，请从快速/最佳/netflow交换变成CEF交换。有启用CEF的一些个警告。当您启用CEF时，下一部分讨论在CEF和快速交换之间的区别，并且解释暗示。

# Cisco 快速转发对快速交换

缓和增加的流量负载的Enable (event) CEF引起由" Code Red "蠕虫病毒。思科IOSÃ¯Â ¿ Â在思科7200/7500/GSR平台的½软件版本

11.1 () CC， 12.0，及以后支持CEF。CEF的支持在其他平台是可用的在Cisco IOS软件版本12.0或以后。您能用软件建议工具进一步调查。

有时，您不能启用在所有路由器的CEF由于这些原因之一：

- 内存不足
- 平台结构不受支持
- 接口封装不受支持

## 快速交换行为及其意义

这是暗示，当您使用快速交换时：

- 流量被驱动的缓存—缓存是空的直到路由器交换机数据包并且填充缓存。
- 第一数据包是交换的进程—，因为缓存是最初空的，第一数据包被过程交换。
- 粒状缓存—缓存被建立在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，缓存用此主要网络的/24s建立。
- 使用/32缓存— /32缓存用于均衡每个目的地的负载。当缓存平衡装载时，缓存用该主网的/32s建立。

  注意： 最后两个问题可能会增加缓存器的利用率，并因此消耗全部内存。

- 在主要网络边界的高速缓冲存储—使用默认路由，缓存在主要网络边界进行。
- 缓存老化器—缓存老化器每分钟运行并且检查1/20th (5百分比)缓存未使用项在正常存储器状况下和1/4 (25百分比)低内存状况的(200k)缓存。

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

- x是秒钟<0-2147483>编号在老化运行之间的。默认= 60秒。
- Y是<2-50>老化的缓存1/(Y+1)每运行(低内存)。默认= 4。
- Z是<3-100>老化的缓存1/(Z+1)每运行(正常)。默认= 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，您的缓存条目年龄的某百分比在您的快速缓存表外面。当快速条目年龄，快速缓存表的大部分老化时和缓存表变得更加小。结果，在路由器的内存消耗量减少。缺点是流量继续为老化在缓存表外面的条目流。初始数据包被过程交换的在被输入的IP的CPU消耗导致一短的尖峰，直到新的缓存条目为流被建立。

从Cisco IOS软件版本10.3(8)， 11.0(3)及以后， IP Cache老化不同处理，如解释此处：

- 只有当service internal命令在配置里，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为0，那么这个老化进程则被完全禁用。
- 时间单位是秒。

注意： 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优点

- 转发信息库(FIB)表根据路由表被构件。所以，在第一数据包转发前，转发信息存在。FIB还包含与直接相连LAN主机相关的/32条目。
- 邻接(ADJ)表包含下一跳和直接连接的主机的(ARP条目Layer2重写信息创建CEF邻接)。
- CEF中不存在使CPU利用率突增的缓存器老化器这一概念。若删除某个路由表条目，则同时会删除FIB条目。

 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。您将需要再手工启用CEF/DCEF。

## 输出示例：CEF

这是若干输出示例: show ip cef summary命令，那显示内存使用。此输出是从Cisco7200路由服务器的一个快照有Cisco IOS软件版本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
```

### 注意事项

当流数量大时， CEF比快速交换典型地浪费较少内存。如果内存由一快速交换缓存已经浪费，您必须清除ARP缓存(通过clear ip arp命令)，在您启用CEF前。

注意： 当您清除缓存时，尖峰的路由器的CPU利用率导致。

## ″ Code Red ″常见问题和他们的答案

### Q. 我使用NAT，并且体验在IP输入的100个CPU利用率百分比。当我执行show proc cpu命令时，我的CPU利用率在中断级别-100/99或99/98很高。这能与″ Code Red ″涉及？

A.那里最近修复介入可扩展性的NAT Cisco Bug (CSCdu63623 (仅限注册用户))。当有数万个NAT流(根据平台类型)， bug导致100个CPU利用率百分比在进程或中断级别。

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，参考故障排除欺骗访问和校正错误。

show ip nat translation命令显示有效转换数量。NPE-300类处理器的熔毁点是大约20,000个到40,000个转换。根据平台变化的此编号。

此熔毁问题由两三客户以前观察，但是在″ Code Red ″以后，更多客户遇到了此问题。唯一的应急方案是运行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. 我运行IRB，并且遇到在HyBridge输入程序的高CPU利用率。为什么会发生这种情况？与″ Code Red ″涉及？

A.HyBridge输入程序处理不可能由IRB进程快速交换的所有数据包。快速交换数据包的IRB进程的无法可以是，由于：

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

如果有千位点对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与IRB ？假设，设备感染″ Code Red ″扫描IP地址。

- 路由器需要发送每目的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。因为数据流是由程序交换的，所以可能会导致高CPU利用率。避免问题，增加过期时间(默认300秒或5分钟)匹配或超出ARP超时(默认4个小时)，以便脚踏两条船者同步。
- 地址终端主机尝试传染是广播地址。路由器进行等同于子网广播的工作，这种工作需要HyBridge输入程序重复。如果no ip directed-broadcast命令配置，这不发生。默认情况下从Cisco IOS软件版本12.0， ip directed-broadcast命令禁用，造成所有IP处理的广播丢弃。
- 这是旁注，无关与″ Code Red ″和相关对IRB体系结构：

  Layer2组播和广播包需要复制。所以，一问题用在广播分段运行的IPX服务器能减少链路。您可通过用户策略来避免这种问题。欲知更多信息，参考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，您能使用多个网桥组，并且保证有BVI、sub-interface和VC的一对一映射。

- 因为RBE完全避免了桥接堆栈，所以要优于IRB。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，并且我接收冲洗，如果我尝试show log。流量速率高于正常也只某种程度。此问题的原因是什么？

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，请证实是否有流量HTTP请求。其次，检查是否有观看特定的IP流与日志关键字的任何访问列表或调试。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。在这种情况下，路由器会禁用中断，并只处理控制台消息。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。这由于″ Code Red ″蠕虫病毒扫描？

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。

## 应急方案

有关“红色代码”，蠕虫的建议 章节介绍了各种临时解决方法。参考应急方案的建议。

阻塞″ Code Red ″蠕虫病毒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，参考使用NBAR和ACL ″ Code Red ″蠕虫在网络入口点的阻塞的。

## 相关信息

- 缓冲泄漏故障排除
- 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
- 故障排除技术说明

---



文件创建日期: 2016 年 10 月 24 日

http://www.cisco.com/cisco/web/support/CN/111/1112/1112206_ts_codred_worm.html