

"Code Red" に起因する mallocfail と高 CPU 利用率への対処法

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[「Code Red」ワームが他のシステムに感染するしくみ](#)

[Code Red ワームに関する警告](#)

[症状](#)

[感染したデバイスの識別](#)

[予防テクニック](#)

[ポート 80 へのトラフィックのブロッキング](#)

[ARP Input のメモリ使用削減](#)

[Cisco Express Forwarding \(CEF \) スイッチングの利用](#)

[Cisco Express Forwarding とファースト スイッチング](#)

[ファースト スイッチングの動作およびその影響](#)

[CEF の利点](#)

[出力例 : CEF](#)

[考慮すべき事柄](#)

[「Code Red」に関する FAQ と回答](#)

[Q. NATを使用して、IP Inputで100 %のCPU使用率が発生しています。show proc cpuを実行すると、CPU使用率が割り込みレベル \(100/99または99/98 \) で高くなります。これは「Code Red」に関連する可能性がありますか。](#)

[Q. IRBを実行していて、HyBridge Inputプロセスで高いCPU使用率が発生しています。なぜ、このような現象が発生するのでしょうか。"これは""Code Red"" に関係しているのでしょうか。"](#)

[CPU 使用率が割り込みレベルで高く、show log を実行するとフラッシュが発生します。トラフィックレートは通常よりもいくらが高だけです。このようになった理由は何ですか。](#)

[Q. ip http-serverを実行しているIOSルータで、多数のHTTP接続試行が見られます。"これは""Code Red"" ワームのスキャンのためでしょうか。"](#)

[回避策](#)

[関連情報](#)

概要

このドキュメントでは、「Code Red」ワームと、このワームがシスコのルーティング環境で引き起こす問題について説明します。このドキュメントでは、ワームの感染を防止する方法について説明し、ワーム関連の問題のソリューションを説明する関連アドバイザリへのリンクを提供します。

「Code Red」ワームは、Microsoft Internet Information Server(IIS)バージョン5.0のインデックスサービスの脆弱性を不正利用します。「Code Red」ワームがホストに感染すると、ランダムな一連のIPアドレスを検出して感染し、ネットワークトラフィックが急増します。これが特に問題になるのは、ネットワーク内に冗長リンクがある場合や、パケットをスイッチングするのに Cisco Express Forwarding (CEF) が使われていない場合です。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「[シスコテクニカルティップスの表記法](#)」を参照してください。

「Code Red」ワームが他のシステムに感染するしくみ

「Code Red」ワームは、ランダムに生成された IP アドレスへの接続を試みます。感染した各 IIS サーバは、同一デバイスセットへの感染を試みる可能性があります。ワームの送信元 IP アドレスおよび TCP ポートは、スプーフィングされていないためトレースが可能です。発信元アドレスは不正なものではないため、Unicast Reverse Path Forwarding (URPF) ではワームの攻撃は抑制できません。

Code Red ワームに関する警告

これらのアドバイザリでは、「Code Red」ワームと、このワームの影響を受けるソフトウェアをパッチする方法について説明します。

- [シスコセキュリティアドバイザリ:"Code Red" ワーム- 顧客への影響](#)
- [Remote IIS Index Server ISAPI Extension Buffer Overflow](#)
- [.ida "Code Red" Worm](#)
- [CERT?Advisory CA-2001-19 「Code Red」ワームによるIISインデックスサービスDLLのバッファオーバーフローの不正利用](#)

症状

Ciscoルータが「Code Red」ワームの影響を受けることを示す症状を次に示します。

- NAT テーブルや PAT テーブル内の大量のフロー (NAT/PAT を使用中の場合)
- ネットワーク内での大量の ARP 要求または ARP ストーム (IP アドレスのスキャンにより発生)
- IP Input、ARP Input、IP Cache Ager、および CEF プロセスによる過剰なメモリ使用
- ARP、IP Input、CEF および IPC での高い CPU 使用率
- NAT を使用中の場合、低いトラフィック レートにおける割り込みレベルで高い CPU 使用率、または IP Input のプロセス レベルでの高い CPU 使用率

メモリが低い状態、または割り込みレベルでCPU使用率(100 %)が持続すると、Cisco IOS[®]ルータがリロードする可能性があります。リロードは、ストレス状態下でのプロセスの誤動作が原因で発生します。

サイトのデバイスが「Code Red」ワームに感染している疑いや、または「Code Red」ワームのターゲットになっている疑いがない場合、「[関連情報](#)」のセクションで、発生する可能性のある問題のトラブルシューティング方法に関する URL を確認してください。

感染したデバイスの識別

フロー スイッチングを使用して、影響を受けたデバイスの送信元 IP アドレスを識別します。すべてのインターフェイス上で ip route-cache flow を設定し、ルータでスイッチングされるフローをすべて記録します。

数分経過してから、show ip cache flow コマンドを実行し、記録されたエントリを表示します。「Code Red」ワーム感染の初期の段階では、ワームは自身の複製を作成しようとします。複製は、ワームが HT 要求をランダムな IP アドレスに送信するときに行われます。したがって、宛先ポートが 80 (HT、16 進数で 0050) のキャッシュ フロー エントリを調べる必要があります。

show ip cache flow | include 0050 コマンドは、TCPポート80 (16進数で0050) のすべてのキャッシュエントリを表示します。

```
Router#show ip cache flow | include 0050
```

```
...
```

scram	scrapers	dative	DstIPAddress	Pr	SrcP	DstP	Pkts
V11	193.23.45.35	V13	2.34.56.12	06	0F9F	0050	2
V11	211.101.189.208	Null	158.36.179.59	06	0457	0050	1
V11	193.23.45.35	V13	34.56.233.233	06	3000	0050	1
V11	61.146.138.212	Null	158.36.175.45	06	B301	0050	1
V11	193.23.45.35	V13	98.64.167.174	06	0EED	0050	1
V11	202.96.242.110	Null	158.36.171.82	06	0E71	0050	1
V11	193.23.45.35	V13	123.231.23.45	06	121F	0050	1
V11	193.23.45.35	V13	9.54.33.121	06	1000	0050	1
V11	193.23.45.35	V13	78.124.65.32	06	09B6	0050	1
V11	24.180.26.253	Null	158.36.179.166	06	1132	0050	1

同じ送信元 IP アドレス、ランダムな宛先 IP アドレス 1、DstP = 0050 (HTTP)、および Pr = 06 (TCP) を持つエントリが異常に多く見つかった場合には、それが感染したデバイスであると思われます。この出力例では、送信元 IP アドレスは 193.23.45.35 であり、VLAN1 から来ています。

- 1 「Code Red II」と呼ばれる「Code Red」の別バージョンが選ぶ宛先 IP アドレスは、完全にランダムではありません。その代わりに、「Code Red II」では IP アドレスのネットワーク部分は維持され、その後の IP ア

ドレスのランダムなホスト部分を選ぶことで拡散します。この場合、ワームが同一ネットワーク内でより速く広まります。

「Code Red II」が使用するネットワークとマスクは次のものです。

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)

除外されるターゲットIPアドレスは127.X.X.Xおよび224.X.X.Xで、オクテットは0または255にすることはできません。さらに、ホストは自身を再感染させようとはしません。

詳細については、『Code Red (II)』を参照してください。

「Code Red」の感染攻撃を検出する netflow を実行できない場合があります。この原因としては、netflow をサポートしていないバージョンのコードが稼働しているか、ルータのメモリが netflow を実行するには少なすぎるか、過度にフラグメント化していることが考えられます。シスコでは、ルータに複数の入カインターフェイスがあり出カインターフェイスが1つだけしかないときには、netflow をイネーブルにしないことを推奨します。これは、netflow アカウンティングは入力パスで行われるためです。この場合、1つしかない出カインターフェイスで IP アカウンティングを有効にするとよいでしょう。

注：ip accounting コマンドは **DCEF** を無効にします。DCEF スイッチングを行う必要があるプラットフォームに対しては、IP アカウンティングをイネーブルにしないでください。

```
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

show ip accounting コマンドの出力の中で、複数の宛先アドレスに対してパケットを送信しようとしている送信元アドレスを探します。感染したホストがスキャンの段階にあるときには、他のルータとの間に HTTP 接続を確立しようとし、そのため、複数の IP アドレスへのアクセス試行が観察されることとなります。これらの接続の試みは、通常はほとんどが失敗します。したがって、実際に転送が観察されるのはバイト数の小さい、少数のパケットだけです。この例では、20.1.145.49 および 20.1.104.194 が感染している可能性があります。

Catalyst 5000 シリーズおよび Catalyst 6000 シリーズで Multi-Layer Switching (MLS; マルチレイ

ヤスイッチング)が稼働中の場合、netflow アカウンティングをイネーブルにするための手順、および感染をトラッキングするためにとる手順は少し異なります。スーパーバイザ 1 Multilayer Switch Feature Card (MSFC1) または Sup1/MSFC2 が備わった Cat6000 スイッチでは、netflow ベースの MLS はデフォルトでイネーブルにされますが、「flow-mode」は「destination-only」です。このため、送信元 IP アドレスはキャッシュに入りません。スーパーバイザで set mls flow full コマンドを使用することで、「full-flow」モードをイネーブルにし、感染したホストのトラッキングに役立てることができます。

ハイブリッドモードの場合は、set mls flow full コマンドを使用します。

```
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.
```

ネイティブ IOS モードの場合は、mls flow ip full コマンドを使用します。

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

「full-flow」モードをイネーブルにすると、MLS エントリの急激な増加に関する警告が表示されます。使用しているネットワークにすでに「Code Red」ワームが拡散している場合は、短期的には急増した MLS エントリによる影響があるのはもっともなことです。ワームによって MLS エントリが極度に増え、さらに増加し続けます。

収集した情報を表示するには、次のコマンドを使用します。

ハイブリッドモードの場合は、set mls flow full コマンドを使用します。

```
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.
```

ネイティブ IOS モードの場合は、mls flow ip full コマンドを使用します。

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

「full-flow」モードをイネーブルにすると、MLS エントリの急激な増加に関する警告が表示されます。使用しているネットワークにすでに「Code Red」ワームが拡散している場合は、短期的には急増した MLS エントリによる影響があるのはもっともなことです。ワームによって MLS エントリが極度に増え、さらに増加し続けます。

収集した情報を表示するには、次のコマンドを使用します。

ハイブリッドモードの場合は、show mls ent コマンドを使用します。

```
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：これらのフィールドは、「full-flow」モードの場合に入力されます。

ネイティブ IOS モードの場合は、show mls ip コマンドを使用します。

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

攻撃に関係する送信元 IP アドレスおよび宛先ポートを判定したら、MLS の設定を「destination-only」モードに戻すことができます。

ハイブリッド モードの場合は、set mls flow destination コマンドを使用します。

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

ネイティブ IOS モードの場合は、mls flow ip destination コマンドを使用します。

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

スーパーバイザ (SUP) II/MSFC2 の組み合わせでは、ハードウェアで CEF スイッチングが実行され、netflow の統計情報が維持されるため、攻撃から防御されます。そのため、「Code Red」の攻撃中であっても、高速なスイッチング メカニズムのおかげで、「full-flow」モードをイネーブルにしてもルータが情報で溢れかえることはありません。「full-flow」モードをイネーブルにし統計を表示するためのコマンドは、SUP I/MSFC1 と SUP II/MSFC2 で同じです。

予防テクニック

このセクションで説明するテクニックを使用して、ルータでの「Code Red」ワームの影響を最小にします。

ポート 80 へのトラフィックのブロック

ネットワークで実行可能な場合、「Code Red」攻撃を防ぐ最も簡単な方法は、WWW 用の Well-Known ポートであるポート 80 へのトラフィックをすべてブロックすることです。ポート 80 宛ての IP パケットを拒否するアクセスリストを作成し、感染ソースに接続されているインターフェイスの着信側にそれを適用します。

ARP Input のメモリ使用削減

次に示すように、スタティック ルートがブロードキャスト インターフェイスを指している場合、ARP Input によって大量のメモリが使用されます。

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

デフォルトルートのすべてのパケットがVLAN3に送信されます。ただし、ネクストホップIPアドレスが指定されていないため、ルータは宛先IPアドレスに対するARP要求を送信します。[Proxy ARP](#) がディセーブルになっていなければ、この宛先に対するネクスト ホップ ルータは、自身の MAC アドレスで応答します。このルータからの応答により、パケットの宛先 IP アドレスがネクストホップ MAC アドレスにマッピングされた追加エントリが ARP テーブルの中に作成されます。「Code Red」ワームはランダムな IP アドレスにパケットを送信します。これによって、ラン

ダムな宛先に対する ARP エントリが新しく追加されます。ARP Input の処理で、これらの新しい ARP エントリによってメモリが次々と消費されます。

インターフェイスに対するデフォルトのスタティック ルートは、特にそのインターフェイスがブロードキャスト (イーサネット、ファスト イーサネット、GE、SMDS) またはマルチポイント (Frame Relay、ATM) の場合には、作成しないでください。デフォルトのスタティック ルートは、ネクストホップ ルータの IP アドレスをポイントする必要があります。デフォルト ルートがネクストホップ IP アドレスをポイントするように変更した後、clear arp-cache コマンドを使って ARP エントリをすべてクリアします。このコマンドにより、メモリ使用率の問題が修正されます。

Cisco Express Forwarding (CEF) スイッチングの利用

IOS ルータでの CPU 使用率を下げるには、Fast、Optimum、または Netflow スイッチングから CEF スイッチングに変更します。CEF をイネーブルにするについては、注意事項がいくつかあります。次のセクションでは、CEF とファスト スイッチングの違い、および CEF をイネーブルにしたときの影響について説明します。

Cisco Express Forwarding とファースト スイッチング

「Code Red」ワームにより引き起こされるトラフィック負荷の増加を軽減するために、CEF をイネーブルにします。Cisco IOS®ソフトウェアリリース11.1()CC、12.0以降では、Cisco 7200/7500/GSRプラットフォームでCEFがサポートされています。他のプラットフォームでは、Cisco IOS ソフトウェア リリース 12.0 以降で CEF がサポートされています。Software Advisor ツールを使用してさらに詳しく調べることができます。

次の理由のいずれかによって、すべてのルータでは CEF をイネーブルにできない場合があります。

- メモリ不足
- サポートされていないプラットフォーム アーキテクチャ
- サポートされていないインターフェイス カプセル化

ファスト スイッチングの動作およびその影響

ファースト スイッチングを使用したときには、次のような影響があります。

- **トラフィック駆動型キャッシュ**：ルータがパケットを切り替え、キャッシュにデータを入力するまで、キャッシュは空になります。
- **最初のパケットはプロセススイッチングされます。**最初のパケットはプロセススイッチングされます。これは、キャッシュが最初は空であるためです。
- **きめ細かいキャッシュ**：キャッシュは、メジャーネットの最も具体的なルーティング情報ベース(RIB)エントリ部分の精度で構築されます。RIB にメジャー ネット 131.108.0.0 用の /24 がある場合、キャッシュはこのメジャー ネットワークに対して /24 で構築される。
- **/32キャッシュが使用される**：/32キャッシュは、各宛先の負荷のバランスをとるために使用されます。キャッシュによって負荷のバランスが取られる場合、キャッシュはメジャー ネットワークに対して /32 で構築される。**注**：これらの最後の2つの問題により、巨大なキャッシュが発生し、すべてのメモリが消費される可能性があります。
- **メジャーネットワーク境界でのキャッシング**：デフォルトルートでは、キャッシングはメジ

ャーネットワーク境界で実行されます。

- Cache Ager:Cache Agerは1分ごとに実行され、通常のメモリ条件下ではキャッシュの1/20(5%)が未使用エントリをチェックし、Low Memory条件(200 k)ではキャッシュの1/4(25%)がチェックされます。

上記の値を変更するには、ip cache-ager-interval X Y Z コマンドを使用します。ここで、

- Xは、agerの実行間隔の秒数(0 ~ 2147483)未満です。デフォルトは 60 秒です。
- Yは、1回の実行 (低メモリ) あたりのキャッシュの1/(Y+1)未満です。デフォルトは 4 です。
- Zは、1回の実行 (通常) につき、キャッシュの1/(Z+1)未満です。デフォルトは 20 です。

次の設定例では、ip cache-ager 60 5 25 を使用しています。

```
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
```

Cache Ager の設定によって、ある程度の率のキャッシュ エントリがファスト キャッシュ テーブルからエージングアウトされます。エントリが迅速にエージングすると、ファスト キャッシュ テーブルでのエージングする割合が大きくなり、キャッシュ テーブルが小さくなります。その結果として、ルータでのメモリ消費が少なくなります。欠点は、キャッシュ テーブルからエージングアウトされたエントリに対してトラフィックが流れ続けることです。最初のパケットはプロセススイッチングされるため、そのフローに対して新しいキャッシュ エントリが構築されるまでは、IP Input での CPU 消費の瞬間的な上昇が発生します。

Cisco IOS ソフトウェア リリース 10.3(8)、11.0(3) 以降では、IP Cache Ager の処理が次のように変更されています。

- ip cache-ager-interval コマンドおよび ip cache-invalidate-delay コマンドは、service internal コマンドが設定内で定義されている場合にだけ使用できます。
- エージャの無効化実行間隔が 0 に設定されている場合、エージャ プロセスは完全に無効化されます。
- 時間は秒で表わされます。

注：これらのコマンドを実行すると、ルータのCPU使用率が増加します。これらのコマンドは、絶対に必要な場合にだけ使用してください。

```
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 の利点

- Forwarding Information Base (FIB; 転送情報ベース) テーブルは、ルーティング テーブルに基づいて作成されます。したがって、最初のパケットが転送される前に転送情報が存在します。FIB には、直接接続された LAN ホストの /32 エントリも含まれます。
- Adjacency (ADJ) テーブルには、ネクストホップおよび直接接続のホストに関するレイヤ 2 リライト情報情報が含まれます。(ARP エントリにより CEF 隣接関係が作成されます)。
- CPU 使用率をスパイクする CEF に関するキャッシュ エージャ コンセプトはありません。ルーティング テーブルのエントリが削除されると、FIB エントリは削除されます。

注意：やはり、ブロードキャストまたはマルチポイントインターフェイスを指すデフォルトルートは、ルータが新しい宛先ごとにARP要求を送信することを意味します。ルータからのARP要求によって、非常に大きな隣接関係テーブルが、ルータがメモリを使い果たすまで作成される可能性があります。CEF がメモリの割り当てに失敗した場合は、CEF/DCEF は自動的にディセーブルになります。CEF/DCEF は手作業で再度イネーブルにする必要があります。

出力例：CEF

show ip cef summary コマンドの出力例を次に示します。これはメモリの使用量を示しています。この出力は、Cisco IOS ソフトウェア リリース 12.0 が稼働している Cisco 7200 ルート サーバからのスナップショットです。

```
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

考慮すべき事柄

大量のフローがある場合、一般的に CEF はファスト スイッチングよりも少ないメモリを消費します。メモリがすでにファスト スイッチング キャッシュによって消費されている場合は、CEF をイネーブルにする前に (clear ip arp で) ARP キャッシュをクリアする必要があります。

注 : キャッシュをクリアすると、ルータのCPU使用率がスパイクします。

「Code Red」に関する FAQ と回答

Q. NATを使用していて、IP Inputで100 %のCPU使用率が発生しています。show proc cpuを実行すると、CPU使用率が割り込みレベル (100/99または99/98) で高くなります。これは「Code Red」に関連する可能性がありますか。

A.最近、スケーラビリティに関するNATのCisco Bug([CSCdu63623](#)(登録ユーザ専用)が修正されました。多数の NAT フローがある場合 (プラットフォームの種類による)、この不具合により、プロセスレベルまたは割り込みレベルで 100 % の CPU 使用率が発生します。

この不具合が原因であるかどうかを判断するには、show align コマンドを発行し、ルータにアラインメント エラーが発生していないかどうかを確認します。アラインメント エラーまたはスプリアス メモリ アクセスが見られる場合には、show align コマンドを 2、3 回発行し、エラーが増加していないか確認します。増加している場合、アラインメント エラーが原因で割り込みレベルでの高い CPU 使用率が発生している可能性があります。不具合 [CSCdu63623](#) (登録ユーザ専用) が原因ではない可能性があります。詳細は、『[トラブルシューティング：スプリアスアクセスとアラインメントエラー](#)』を参照してください。

show ip nat translation コマンドを発行すると、アクティブな変換の数が表示されます。NPE-300 クラス プロセッサのメルトダウン ポイントは、約 20,000 ～ 40,000 の変換です。この数字は、プラットフォームによって異なります。

このメルトダウン問題は、以前にも少数のお客様で見られていましたが、「Code Red」の発生以来、この問題に遭遇するお客様が増加しています。唯一の回避策は、NAT (PAT の代わりに) を実行することであり、これによりアクティブな変換は少なくなります。7200 を使用している場合には、NSE-1 を使用し、NAT タイムアウト値を低くします。

Q. IRBを実行していて、HyBridge Inputプロセスで高いCPU使用率が発生しています。なぜ、このような現象が発生するのでしょうか。"これは""Code Red"" に関係しているのでしょうか。"

A. HyBridge Inputプロセスは、IRBプロセスでファーストスイッチングできないパケットを処理します。IRB プロセスでパケットをファースト スイッチングできない理由としては、次のものがあります。

- パケットがブロードキャスト パケットである。
- パケットがマルチキャスト パケットである。
- 宛先が不明で、ARP をトリガーする必要がある。
- スパニング ツリー BPDU がある。

同一ブリッジ グループ内に膨大なポイントツーポイント インターフェイスがあると、HyBridge Input で問題が発生します。また、同一のマルチポイント インターフェイス内に膨大な VS がある場合にも問題が起こりますが、より小規模です。

IRB における問題の理由としてどのようなことが考えられるでしょうか。たとえば、「Code Red」により感染したデバイスが IP アドレスをスキャンしていると仮定します。

- ルータは各送信先 IP アドレスに対して ARP 要求を送信する必要があります。このため、スキャンされる各アドレスごとに、ブリッジ グループ内の各 VC に対して大量の ARP 要求が発生します。通常の ARP プロセスでは CPU の問題は発生しません。しかし、ARP エントリがあって、ブリッジ エントリがない場合には、ルータでは ARP エントリがすでに存在する

アドレス宛てのパケットのフラッディングが発生します。トラフィックのプロセススイッチングされるため、これは高い CPU 使用率を引き起こす可能性があります。この問題を避けるためには、ARP のタイムアウト (デフォルトは 4 時間) と同等以上になるようにブリッジのエージング時間 (デフォルトは 300 秒、つまり 5 分) を増やして、2 つのタイマーが同期するようにします。

- エンドホストが感染させようとしているアドレスがブロードキャストアドレスに該当する場合、ルータは、HyBridge Input プロセスによって複製の必要があるサブネットブロードキャストと同等のを行います。no ip directed-broadcast が設定されている場合には、これは発生しません。Cisco IOS ソフトウェア リリース 12.0 以降では、ip directed-broadcast コマンドはデフォルトでディセーブルになっており、これにより IP ディレクテッドブロードキャストはすべてドロップされます。
- 「Code Red」に関係しない、IRB アーキテクチャに関するサイドノート：レイヤ 2 マルチキャストおよびブロードキャストパケットは複製の必要があります。そのため、ブロードキャストセグメントで稼働する IPX サーバによってリンクをダウンさせるような問題が発生する場合があります。サブスクリバポリシーを使ってこの問題を避けることができます。詳細については、『[x デジタル加入者線 \(xDSL \) ブリッジ サポート](#)』を参照してください。その他にブリッジアクセスリストを検討する必要があります。これはルータを通過させるトラフィックの種類を制限します。
- この IRB 問題は、複数のブリッジグループを使用し、BVI、サブインターフェイス、および VC を 1 対 1 にマッピングさせることで軽減できます。
- RBE はブリッジングスタックを完全に回避するため、IRB よりも優れています。IRB から RBE に移行できます。移行を促進する根拠となる不具合には次のものがあります。
[CSCdr11146](#) ([登録ユーザ専用](#)) [CSCdp18572](#) ([登録ユーザ専用](#)) [CSCds40806](#) ([登録ユーザ専用](#))

CPU 使用率が割り込みレベルで高く、show log を実行するとフラッシュが発生します。トラフィックレートは通常よりもいくらか高いだけです。このようになった理由は何ですか。

A. show logging コマンドの出力例を次に示します。

```
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
```

コンソールにログインしていることを確認します。ログインしている場合は、HTTP リクエストトラフィックがあることを確認します。次に、ログキーワードがあるアクセスリストまたは特定の IP フローを監視しているデバッグがあるかどうかを確認します。フラッシュが増加している場合、それはおそらくコンソール (通常は 9600 ボーのデバイス) で、受信した大量の情報を処理できなくなっていることが原因である可能性があります。このような場合、ルータは割り込みを無効化し、コンソールメッセージの処理以外何も行いません。ソリューションは、コンソールのロギングをディセーブルにするか、実行しているあらゆる種類のロギングをすべて取り除くことです。

Q. ip http-server を実行している IOS ルータで、多数の HTTP 接続試行が見られます。"これは ""Code Red"" ワームのスキャンのためでしょうか。"

A. 「Code Red」が原因である可能性があります。シスコでは、IOS ルータで ip http server コマンドをディセーブルにして、感染したホストからの対象の接続試行に対応しないようにすることをお勧めします。

回避策

「[「Code Red」ワームに関するアドバイザリ](#)」のセクションでは、さまざまな回避策を取り上げています。これらのアドバイザリを参照して回避策を探してください。

ネットワーク入力ポイントで「Code Red」ワームをブロックする別の方法では、シスコ ルータで IOS ソフトウェアの Network-Based Application Recognition (NBAR) および Access Control List (ACL; アクセスコントロール リスト) を使用します。この方式は、Microsoft から提供されている IIS サーバ用推奨パッチと一緒に使用してください。この方式に関する詳細は、『[ネットワークの入口で「Code Red」ワームをブロックするための NBAR および ACL の使用方法](#)』を参照してください。

関連情報

- [メモリの問題に関するトラブルシューティング](#)
- [バッファリークのトラブルシューティング](#)
- [Cisco ルータの CPU 使用率が高い場合のトラブルシューティング](#)
- [トラブルシューティング : ルータのクラッシュ](#)
- [トラブルシューティング テクニカル ノート - ルータ](#)
- [ルータのトラブルシューティング](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)