"코드 레드(Code Red)" WORM으로 인한 악성코드 및 높은 CPU 사용률 처리

목차

소개

이 문서에서는 Cisco 라우팅 환경에서 "코드 레드(Code Red)" 지렁이와 worm이 일으킬 수 있는 문제에 대해 설명합니다.이 문서에서는 WORM(Worm Inflection)을 방지하는 기술에 대해 설명하고, WORM(Worm-Related Problems)과 관련된 해결책을 설명하는 관련 권고 사항에 대한 링크를 제공합니다.

"Code Red(코드 레드)" worm은 Microsoft IIS(Internet Information Server) 버전 5.0의 Index Service에서 취약성을 악용합니다. "코드 레드(Code Red)" 지렁이가 호스트를 감염하면 호스트가 임의의 일련의 IP 주소를 조사하고 감염시켜 네트워크 트래픽이 급격히 증가합니다.이는 특히 네트워크에 이중화 링크가 있거나 CEF(Cisco Express Forwarding)를 사용하여 패킷을 전환하지 않을 경우 문제가 됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

"코드 레드" WORM이 다른 시스템을 감염시키는 방법

"Code Red(코드 레드)" worm은 임의로 생성된 IP 주소에 연결하려고 시도합니다.감염된 모든 IIS 서버는 동일한 장치 집합을 감염시키려고 시도할 수 있습니다.스푸핑되지 않으므로 이 WORM의 소스 IP 주소와 TCP 포트를 추적할 수 있습니다.소스 주소가 합법이므로 URPF(유니캐스트 역방향 경로 전달)에서 WORM 공격을 억제할 수 없습니다.

"코드 레드(Code Red)" WORM을 설명하는 권고 사항

이러한 권고는 "Code Red(코드 레드)" WORM에 대해 설명하고, WORM의 영향을 받는 소프트웨어를 패치하는 방법에 대해 설명합니다.

- Cisco 보안 자문:"코드 레드" WORM - 고객 영향
- 원격 IIS 인덱스 서버 ISAPI 확장 버퍼 오버플로
- .ida "코드 레드" Worm
- 인증서?IIS 인덱싱 서비스 DLL의 자문 CA-2001-19 "코드 빨강" WORM 버퍼 오버플로

증상

다음은 Cisco 라우터가 "Code Red(코드 레드)" 지렁이의 영향을 받는다는 몇 가지 증상의 예입니다.

- NAT 또는 PAT 테이블의 많은 플로우(NAT 또는 PAT를 사용하는 경우)

- 네트워크에서 많은 ARP 요청 또는 ARP 스톰(IP 주소 스캔으로 인해 발생)
- IP 입력, ARP 입력, IP 캐시 관리자 및 CEF 프로세스에서 과도한 메모리 사용
- ARP, IP 입력, CEF 및 IPC의 높은 CPU 사용률
- NAT를 사용하는 경우 낮은 트래픽 속도로 인터럽트 레벨에서 높은 CPU 사용률 또는 IP 입력의 프로세스 레벨에서 높은 CPU 사용률.

메모리 부족 상태 또는 인터럽트 레벨에서 높은 CPU 사용률(100%)을 유지하면 Cisco IOS® 라우터가 다시 로드될 수 있습니다.다시 로드는 스트레스 조건으로 인해 잘못된 프로세스가 원인입니다.

사이트의 디바이스가 "코드 레드(Code Red)" WORM에 감염되었거나 그 대상이라고 의심하지 않는 경우 발생하는 문제를 해결하는 방법에 대한 추가 URL은 관련 정보 섹션을 참조하십시오.

감염된 디바이스 식별

흐름 전환을 사용하여 영향을 받는 디바이스의 소스 IP 주소를 식별합니다.모든 인터페이스**에서** ip route**-cache 흐름**을 구성하여 라우터가 전환한 모든 흐름을 기록합니다.

몇 분 후, show ip cache flow **명령**을 실행하여 기록된 항목을 확인합니다."코드 레드" 벌레의 초기 단계 동안, 벌레는 자신을 복제하려고 시도합니다.복제는 worm이 HT 요청을 임의 IP 주소로 전송할 때 발생합니다.따라서 대상 포트 80(HT, 0050(16진수)이 있는 캐시 흐름 엔트리를 찾아야 합니다.

show **ip cache flow | include 0050** 명령은 TCP 포트 80(16진수 0050)이 있는 모든 캐시 항목을 표시합니다.

```
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
```

동일한 소스 IP 주소, 임의 대상 IP 주소[1], DstP = 0050(HTTP) 및 Pr = 06(TCP)의 항목 수가 비정상적으로 많은 경우 감염된 디바이스를 찾은 것 같습니다.이 출력 예에서 소스 IP 주소는 193.23.45.35이며 VLAN1에서 가져옵니다.

[1] "Code Red II"라는 "Code Red" worm의 다른 버전은 완전히 임의의 대상 IP 주소를 선택하지 않습니다.대신 "Code Red II"는 IP 주소의 네트워크 부분을 유지하고 전파하기 위해 IP 주소의 임의 호스트 부분을 선택합니다.이를 통해 WORM은 동일한 네트워크 내에서 더 빨리 확산됩니다.

"코드 레드 II"는 다음 네트워크와 마스크를 사용합니다.

```
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)
```
제외된 대상 IP 주소는 127.X.X.X 및 224.X.X.X이며 8진수는 0 또는 255가 될 수 없습니다. 또한 호스트는 자체 감염을 시도하지 않습니다.

자세한 내용은 코드 레드(II)를 참조하십시오 .

때때로 netflow를 실행하여 "코드 레드(Code Red)" 침입 시도를 탐지할 수 없습니다.이는 netflow를 지원하지 않는 코드 버전을 실행하거나 라우터에 netflow를 활성화하기 위한 메모리가 부족하거나 과도하게 조각화된 메모리가 있기 때문일 수 있습니다.인그레스 경로에서 netflow 어카운팅이 수행되므로, 여러 인그레스 인터페이스가 있고 라우터에 이그레스 인터페이스가 하나만 있는 경우 netflow를 활성화하지 않는 것이 좋습니다.이 경우 단독 이그레스 인터페이스에서 IP 어카운팅을 활성화하는 것이 좋습니다.

참고: ip accounting **명령**은 DCEF를 비활성화합니다.DCEF 스위칭을 사용하려는 플랫폼에서 IP 어카운팅을 활성화하지 마십시오.

```
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 명령 출력에서 여러 목적지 주소로 패킷을 전송하려고 시도하는 소스 주소를 찾습니다.감염된 호스트가 스캔 단계에 있으면 다른 라우터에 대한 HTTP 연결을 설정하려고 시도합니다.따라서 여러 IP 주소에 연결하려는 시도가 표시됩니다.이러한 연결 시도 대부분은 일반적으로 실패합니다.따라서 전송된 패킷 수가 적지만 각 패킷은 작은 바이트 수로 표시됩니다.이 예에서는 20.1.145.49 및 20.1.104.194이 감염되었을 가능성이 높습니다.

Catalyst 5000 Series 및 Catalyst 6000 Series에서 MLS(Multi-Layer Switching)를 실행할 경우, Netflow 어카운팅을 활성화하고 침입을 추적하려면 다른 단계를 수행해야 합니다.Supervisor 1 MSFC1(Multilayer Switch Feature Card) 또는 SUP I/MSFC2가 장착된 Cat6000 스위치에서는 기본적으로 netflow 기반 MLS가 활성화되지만 flow-mode는 destination-only입니다.따라서 소스 IP 주소는 캐시되지 않습니다.수퍼바이저에서 set mls flow full **명령**의 도움을 받아 감염된 호스트를 추적하려면 "full-flow" 모드를 활성화할 수 있습니다.

하이브리드 모드의 경우 set mls flow **full** 명령을 사용합니다.

```
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.
```

네이티브 IOS 모드의 경우 mls flow ip full **명령을** 사용합니다.

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

"full-flow" 모드를 활성화하면 MLS 항목의 급격한 증가를 나타내는 경고가 표시됩니다.네트워크가 이미 "코드 레드(Code Red)" 지렁이 감염된 경우 MLS 항목이 증가하면 짧은 기간 동안 영향이 발생합니다.이 지렁이는 MLS 엔트리를 과도하게 증가시킵니다.

수집된 정보를 보려면 다음 명령을 사용합니다.

하이브리드 모드의 경우 set mls flow **full** 명령을 사용합니다.

```
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.
```

네이티브 IOS 모드의 경우 mls **flow ip full** 명령을 사용합니다.

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

"full-flow" 모드를 활성화하면 MLS 항목의 급격한 증가를 나타내는 경고가 표시됩니다.네트워크가 이미 "코드 레드(Code Red)" 지렁이 감염된 경우 MLS 항목이 증가하면 짧은 기간 동안 영향이 발생합니다.이 지렁이는 MLS 엔트리를 과도하게 증가시킵니다.

수집된 정보를 보려면 다음 명령을 사용합니다.

하이브리드 모드의 경우 show mls ent **명령을** 사용합니다.

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

참고: 이 모든 필드는 "전체 흐름" 모드에 있을 때 채워집니다.

네이티브 IOS 모드의 경우 show mls **ip** 명령을 사용합니다.

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

공격과 관련된 소스 IP 주소 및 대상 포트를 결정할 때 MLS를 다시 "대상 전용" 모드로 설정할 수 있습니다.

하이브리드 모드의 경우 set mls flow destination **명령**을 사용합니다.

```
6500-sup(enable) set mls flow destination
```

```
Usage: set mls flow <destination|destination-source|full>
```
네이티브 IOS 모드의 경우 mls flow ip destination 명령을 사용합니다.

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

CEF 스위칭은 하드웨어에서 수행되고 netflow 통계는 유지되므로 SUP(Supervisor) II/MSFC2 조합은 공격으로부터 보호됩니다.따라서 "코드 레드(Code Red)" 공격 중에도 풀 플로우 모드를 활성화하면 더 빠른 스위칭 메커니즘으로 인해 라우터가 오버플되지 않습니다.전체 흐름 모드를 활성화하고 통계를 표시하는 명령은 SUP I/MFSC1과 SUP II/MSFC2에서 모두 동일합니다.

방지 기법

라우터에 "Code Red(코드 레드)" 벌레가 미치는 영향을 최소화하려면 이 섹션에 나열된 기술을 사용합니다.

포트 80에 대한 트래픽 차단

네트워크에서 실행 가능한 경우 "코드 레드(Code Red)" 공격을 방지하는 가장 쉬운 방법은 WWW의 잘 알려진 포트인 포트 80에 대한 모든 트래픽을 차단하는 것입니다.포트 80으로 향하는 IP 패킷을 거부하고 감염 소스가 있는 인터페이스에 이를 적용하려면 액세스 목록을 구축합니다.

ARP 입력 메모리 사용량 감소

ARP 입력은 고정 경로가 다음과 같이 브로드캐스트 인터페이스를 가리키면 대량의 메모리를 사용합니다.

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```
기본 경로에 대한 모든 패킷은 VLAN3으로 전송됩니다. 그러나 다음 홉의 IP 주소가 지정되지 않았으므로 라우터는 대상 IP 주소에 대한 ARP 요청을 전송합니다.프록시 ARP가 비활성화되지 않는 한, 해당 대상의 다음 홉라우터는 자체 MAC 주소로 응답합니다.라우터의 회신은 패킷의 대상 IP 주소가 next-hop MAC 주소에 매핑되는 ARP 테이블에 추가 항목을 생성합니다."Code Red(코드 레드)" worm은 임의의 IP 주소로 패킷을 전송하며, 각 임의 대상 주소에 대해 새 ARP 항목을 추가합니다.새로운 각 ARP 항목은 ARP 입력 프로세스에서 점점 더 많은 메모리를 소비합니다.

인터페이스에 대한 고정 기본 경로를 만들지 마십시오. 특히 인터페이스가 브로드캐스트(Ethernet/Fast Ethernet/GE/SMDS) 또는 다중 지점(Frame Relay/ATM)인 경우 이 경로를 생성하지 마십시오. 고정 기본 경로는 다음 hop 라우터의 IP 주소를 가리켜야 합니다.기본 경로를 다음 hop IP 주소를 가리키도록 변경한 후 clear arp-cache 명령을 사용하여 모든 ARP 항목을 지웁니다.이 명령은 메모리 사용률 문제를 해결합니다.

Cisco CEF(Express Forwarding) 스위칭 사용

IOS 라우터에서 CPU 사용률을 낮추려면 Fast/Optimization/Netflow 스위칭에서 CEF 스위칭으로 변경합니다.CEF를 활성화하는 몇 가지 주의사항이 있습니다.다음 섹션에서는 CEF와 고속 스위칭의 차이점에 대해 설명하고 CEF를 활성화할 때의 영향에 대해 설명합니다.

Cisco Express Forwarding과 Fast Switching 비교

"Code Red(코드 레드)" worm으로 인해 증가하는 트래픽 로드를 완화하려면 CEF를 활성화합니다 .Cisco IOS® Software 릴리스 11.1( )CC, 12.0 이상에서는 Cisco 7200/7500/GSR 플랫폼에서 CEF를 지원합니다.다른 플랫폼에서 CEF에 대한 지원은 Cisco IOS Software 릴리스 12.0 이상에서 제공됩니다.Software Advisor 툴을 사용하여 더 자세히 조사할 수 있습니다.

다음 이유 중 하나로 인해 모든 라우터에서 CEF를 활성화할 수 없는 경우가 있습니다.

- 메모리 부족
- 지원되지 않는 플랫폼 아키텍처
- 지원되지 않는 인터페이스 캡슐화

빠른 스위칭 동작 및 의미

고속 스위칭을 사용할 때 다음과 같은 영향이 발생합니다.

- Traffic driven cache(트래픽 제어 캐시) - 라우터가 패킷을 전환하고 캐시를 채울 때까지 캐시는 비어 있습니다.
- 첫 번째 패킷은 프로세스 스위칭됨 - 처음에 캐시가 비어 있기 때문에 첫 번째 패킷은 프로세스 스위칭됩니다.
- 세분화된 캐시 - 캐시는 주 네트에서 가장 구체적인 RIB(Routing Information Base) 엔트리 부분에 세분화하여 구축됩니다.RIB에 주요 네트 131.108.0.0에 대해 /24s가 있는 경우 캐시는 이 주요 네트워크에 대해 /24s로 빌드됩니다.
- /32 캐시가 사용됨—/32 캐시가 각 대상에 대한 로드 밸런싱을 위해 사용됩니다.캐시가 로드 밸런싱되면 해당 주 네트워크에 대해 /32s로 캐시가 구축됩니다.**참고:** 마지막 두 가지 문제로 인해 모든 메모리를 사용하는 대용량 캐시가 발생할 수 있습니다.
- 주요 네트워크 경계에서 캐싱 - 기본 경로를 사용하면 주요 네트워크 경계에서 캐싱이 수행됩니다.
- 캐시 관리자 - 캐시 관리자는 매분마다 실행되며, 일반 메모리 조건에서 사용되지 않는 엔트리를 캐시의 1/20(5%), 낮은 메모리 조건에서 캐시의 1/4(25%)를 확인합니다(200k).

위의 값을 변경하려면 **ip cache-ager-interval X Y Z** 명령을 사용합니다. 여기서

- X는 관리자 실행 사이의 시간(초)입니다.기본값은 60초입니다.
- Y는 실행당 에이징할 캐시(메모리 부족)가 2-50> 1/(Y+1)입니다. 기본값 = 4.
- Z는 실행당 에이징(보통)할 캐시의 <3-100> 1/(Z+1)입니다. 기본값은 20입니다.

다음은 **ip cache-ager 60 5 25를** 사용하는 샘플 컨피그레이션입니다.

```
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
```

캐시 관리자의 설정에 따라 캐시 항목 중 일부 백분율이 빠른 캐시 테이블에서 사용 기간이 지납니다.항목이 빠르게 오래되면 빠른 캐시 테이블 사용 기간이 더 많아지고 캐시 테이블이 작아집니다.결과적으로 라우터의 메모리 소비가 감소합니다.단점은 캐시 테이블에서 오래된 항목에 대한 트래픽이 계속 흐른다는 것입니다.초기 패킷은 프로세스 스위칭으로, 플로우에 대해 새 캐시 엔트리가 작성될 때까지 **IP 입력**의 CPU 소비가 짧습니다.

Cisco IOS Software Release 10.3(8), 11.0(3) 이상에서 IP 캐시 관리자는 다음과 같이 다르게 처리됩니다.

- ip **cache-ager-interval** 및 **ip cache-invalidate-delay** 명령은 **service internal** 명령이 컨피그레이션에 정의된 경우에만 사용할 수 있습니다.
- 관리자 무효화 실행 사이의 기간이 0으로 설정된 경우 관리자 프로세스가 완전히 비활성화됩니다.
- 시간은 초 단위로 표시됩니다.

참고: 이러한 명령을 실행하면 라우터의 CPU 사용률이 증가합니다.반드시 필요한 경우에만 이 명령을 사용하십시오.

```
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
```

CEF의 장점

- FIB(Forwarding Information Base) 테이블은 라우팅 테이블을 기반으로 작성됩니다.따라서 첫 번째 패킷이 전달되기 전에 전달 정보가 존재합니다.FIB에는 직접 연결된 LAN 호스트에 대한 /32개의 항목도 포함되어 있습니다.
- ADJ(Adjacency) 테이블에는 다음 홉과 직접 연결된 호스트에 대한 레이어 2 재작성 정보가 포함됩니다(ARP 항목은 CEF 인접성을 생성합니다).
- CPU 사용률을 높이기 위해 CEF를 사용하는 캐시 관리자 개념은 없습니다.라우팅 테이블 항목이 삭제되면 FIB 항목이 삭제됩니다.

주의: 다시, 브로드캐스트 또는 멀티포인트 인터페이스를 가리키는 기본 경로는 라우터가 모든 새 대상에 대해 ARP 요청을 전송함을 의미합니다.라우터의 ARP 요청은 라우터의 메모리가 부족해질 때까지 거대한 인접성 테이블을 생성합니다.CEF가 메모리를 할당하지 못하면 CEF/DCEF는 자체 설정을 비활성화합니다.CEF/DCEF를 다시 수동으로 활성화해야 합니다.

샘플 출력:CEF

다음은 show ip cef summary **명령**의 샘플 출력으로서 메모리 사용량을 보여 줍니다.이 출력은 Cisco IOS Software Release 12.0이 포함된 Cisco 7200 경로 서버의 스냅샷입니다.

```
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
```

고려해야 할 사항

플로우 수가 많으면 CEF는 일반적으로 빠른 스위칭보다 메모리를 적게 사용합니다.빠른 스위칭 캐시에서 메모리를 이미 사용하고 있는 경우 CEF를 활성화하기 전에 **clear ip arp** 명령을 통해 ARP 캐시를 지워야 합니다.

참고: 캐시를 지우면 라우터의 CPU 사용률이 증가합니다.

"코드 레드" 자주 묻는 질문과 대답

Q. NAT를 사용하며 IP 입력에서 100% CPU 사용률을 경험합니다.show proc cpu를 실행하면 CPU 사용률이 인터럽트 수준(100/99 또는 99/98)에서 높습니다. "코드 레드"와 관련될 수 있습니까?

A. 최근 확장성과 관련된 NAT Cisco 버그(CSCdu63623(등록된 고객만 해당)가 수정되었습니다.플랫폼 유형에 따라 수만 개의 NAT 플로우가 있는 경우, 버그로 인해 프로세스 또는 인터럽트 레벨에서 100% CPU 사용률이 발생합니다.

이 버그가 원인인지 확인하려면 **show align** 명령을 실행하고 라우터가 정렬 오류를 경험하는지 확인합니다.정렬 오류나 잘못된 메모리 액세스가 표시되는 경우 **show align** 명령을 몇 번 실행하여 오류가 증가하는지 확인합니다.오류 수가 증가하면 정렬 오류는 인터럽트 레벨에서 높은 CPU 사용률이 발생하는 원인일 수 있으며 Cisco 버그 CSCdu63623(등록된 고객만 해당)는 아닙니다. 자세한 내용은 Troubleshooting Verius Access and Alignment Errors(잘못된 액세스 및 정렬 오류 문제 해결)를 참조하십시오.

show **ip nat translation** 명령은 활성 변환 수를 표시합니다.NPE-300 클래스 프로세서의 용해 지점은 약 20,000~40,000개의 번역입니다.이 번호는 플랫폼에 따라 다릅니다.

이 노심 용해 문제는 이전에 몇 명의 고객으로부터 관찰되었지만 "코드 레드" 이후 더 많은 고객이 이 문제를 경험했습니다.유일한 해결 방법은 PAT 대신 NAT를 실행하여 활성 변환이 더 적도록 하는 것입니다.7200이 있는 경우 NSE-1을 사용하고 NAT 시간 초과 값을 낮춥니다.

Q. IRB를 실행하며 HyBridge 입력 프로세스에서 CPU 사용률이 높습니다.왜 이런 일이 발생할까요?"코드 레드"와 관련이 있습니까?

A. HyBridge 입력 프로세스는 IRB 프로세스에서 빠르게 전환할 수 없는 모든 패킷을 처리합니다

.IRB 프로세스에서 패킷을 빠르게 전환할 수 없는 이유는 다음과 같습니다.

- 패킷은 브로드캐스트 패킷입니다.
- 패킷은 멀티캐스트 패킷입니다.
- 대상을 알 수 없으므로 ARP를 트리거해야 합니다.
- 스패닝 트리 BPDU가 있습니다.

HyBridge Input은 동일한 브리지 그룹에 수천 개의 포인트-투-포인트 인터페이스가 있는 경우 문제가 발생합니다.또한 동일한 다중 지점 인터페이스에 수천 개의 VS가 있는 경우 HyBridge Input에 문제가 발생하지만 그보다 작은 범위까지 발생합니다.

IRB와 관련된 문제의 가능한 원인은 무엇입니까?"코드 레드"에 감염된 디바이스가 IP 주소를 스캔한다고 가정합니다.

- 라우터는 각 대상 IP 주소에 대해 ARP 요청을 보내야 합니다.스캔되는 각 주소에 대해 브리지 그룹의 모든 VC에 대한 ARP 요청이 쇄도합니다.일반 ARP 프로세스에서는 CPU 문제를 일으키지 않습니다.그러나 브리지 엔트리가 없는 ARP 엔트리가 있는 경우 라우터는 ARP 엔트리가 이미 존재하는 주소로 향하는 패킷을 플러딩합니다.이 경우 트래픽이 프로세스 스위칭되므로 CPU 사용률이 높을 수 있습니다.이 문제를 방지하려면 두 타이머가 동기화되도록 ARP 시간 초과(기본값: 300초 또는 5분)를 매칭하거나 초과하도록 브리지 에이징 시간(기본값 300초 또는 5분)을 늘립니다.
- 엔드 호스트가 감염하려고 시도하는 주소는 브로드캐스트 주소입니다.라우터는 HyBridge 입력 프로세스에서 복제해야 하는 서브넷 브로드캐스트와 동일합니다.**no ip directed-broadcast** 명령이 구성된 경우 이는 발생하지 않습니다.Cisco IOS Software Release 12.0에서 **ip directed-broadcast** 명령은 기본적으로 비활성화되어 모든 IP-directed 브로드캐스트가 삭제됩니다.
- 다음은 "Code Red"와 관련이 없고 IRB 아키텍처와 관련된 참고 사항입니다.레이어 2 멀티캐스트 및 브로드캐스트 패킷을 복제해야 합니다.따라서 브로드캐스트 세그먼트에서 실행되는 IPX 서버에 문제가 발생하면 링크가 다운될 수 있습니다.가입자 정책을 사용하여 문제를 방지할 수 있습니다.자세한 내용은 x Digital Subscriber Line (xDSL) Bridge Support(x 디지털 가입자 회선) 브리지 지원)를 참조하십시오.또한, 라우터를 통과할 수 있는 트래픽 유형을 제한하는 브리지 액세스 목록을 고려해야 합니다.
- 이 IRB 문제를 완화하기 위해 여러 브리지 그룹을 사용할 수 있으며 BVI, 하위 인터페이스 및 VC에 대해 일대일 매핑이 있는지 확인할 수 있습니다.
- RBE는 브리징 스택을 모두 피하므로 IRB보다 우수합니다.IRB에서 RBE로 마이그레이션할 수 있습니다.이러한 Cisco 버그를 통해 이러한 마이그레이션을 유도합니다.CSCdr11146(등록된 고객만 해당)CSCdp18572(등록된 고객만 해당)CSCds40806(등록된 고객만 해당)

Q: 내 CPU 사용률이 인터럽트 레벨에서 높으며, show log를 시도하면 플러시를 받습니다.트래픽 속도도 정상보다 약간 더 높습니다.이유가 뭐죠?

A. 다음은 **show logging** 명령 출력의 예입니다.

```
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
```

콘솔에 로그인하는지 확인합니다.그렇다면 트래픽 HTTP 요청이 있는지 확인합니다.다음으로, 특정 IP 흐름을 감시하는 로그 키워드 또는 디버그가 있는 액세스 목록이 있는지 확인합니다.플러시가

증가하면 일반적으로 9600 보드 디바이스인 콘솔이 수신한 정보의 양을 처리할 수 없기 때문일 수 있습니다.이 시나리오에서는 라우터가 인터럽트를 비활성화하고 콘솔 메시지를 처리하는 것만 수행합니다.해결 방법은 콘솔 로깅을 비활성화하거나 수행하는 로깅 유형을 제거하는 것입니다.

Q. IP http-server를 실행하는 IOS 라우터에서 수많은 HTTP 연결 시도를 볼 수 있습니다."코드 레드" 지렁이 스캔 때문인가요?

A. "코드 레드"는 여기에 이유가 될 수 있습니다.Cisco는 IOS 라우터에서 **ip http server** 명령을 비활성화하여 감염된 호스트의 수많은 연결 시도를 처리할 필요가 없도록 하는 것이 좋습니다.

해결 방법

Advisories(권장 사항)에서 "Code Red(코드 레드)" Worm 섹션에 대해 설명하는 다양한 해결 방법이 있습니다.해결 방법은 권장 사항을 참조하십시오.

네트워크 인그레스 포인트에서 "코드 레드(Code Red)" WORM을 차단하는 또 다른 방법은 Cisco 라우터의 IOS 소프트웨어 내에서 NBAR(Network-Based Application Recognition) 및 ACL(Access Control Lists)을 사용합니다.이 방법을 Microsoft의 IIS 서버에 권장되는 패치와 함께 사용합니다.이 방법에 대한 자세한 내용은 Using NBAR and ACLs for Blocking the "Code Red" Worm at Network Ingress Points를 참조하십시오.

관련 정보

- 메모리 문제 해결
- 버퍼 누수 문제 해결
- Cisco 라우터의 높은 CPU 사용률 문제 해결
- 라우터 충돌 트러블슈팅
- 문제 해결 TechNotes - 라우터
- 라우터 문제 해결
- 기술 지원 및 문서 – Cisco Systems