Решение проблем Mallocfail и высокого уровня загрузки CPU, возникающих вследствие работы червя Code Red

Содержание

Введение

Этот документ описывает червя "Code Red" и проблемы, которые червь может вызвать в

среде маршрутизации Cisco. Этот документ также описывает способы для предотвращения инвазии червя и предоставляет ссылки на связанные информационные сообщения, которые описывают решения для связанных с червем проблем.

Вирус паразит "Code Red", использует уязвимость в Обслуживании Индекса, Microsoft Internet Information Server (IIS) версии 5.0. Когда червь "Code Red" заражает хост, он заставляет хост зондировать и заражать случайный ряд IP-адресов, который вызывает резкое увеличение в сетевом трафике. Это особенно проблематично при наличии избыточных ссылок в сети и / или Cisco Express Forwarding (CEF) не используется для переключения пакетов.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Как червь "Code Red" заражает другие системы

Червь "Code Red" пытается подключиться к случайно созданным IP-адресам. Каждый зараженный сервер IIS может попытаться заразить тот же набор устройств. Можно отследить IP - адреса источника и порт TCP червя, потому что это не имитируется. Одноадресная пересылка по обратному пути (uRPF) не может подавить атаку червя, потому что адрес источника законен.

Справочные материалы по червю Code Red

Эти информационные сообщения описывают червя "Code Red" и объясняют, как исправить программное обеспечение, на которое влияет червь:

- Рекомендация по вопросам безопасности: Червь "Code Red" - последствия для клиентов
- Переполнение буфера расширения ISAPI удаленного сервера индексирования IIS

- червь .ida "Code Red"
- CERT? Консультативный червь "Code Red" CA-2001-19, использующий переполнение буфера в DLL сервиса индексации IIS

Признаки

Вот некоторые признаки, которые указывают, что на маршрутизатор Cisco влияет червь "Code Red":

- Большое число потоков в NAT или Таблицах PAT (если вы используете NAT или PAT).
- Огромное количество ARP запросов, или ARP аттак в сети (вызванные сканированием IP-адресов).
- Чрезмерное использование памяти IP Input, ARP Input, IP Cash Ager и CEF процессов.
- Высокая загрузка ЦП в ARP, Ввод IP, CEF и IPC.
- Высокая загрузка ЦП в Interrupt Levels на скоростях низкого трафика или высокая загрузка ЦП в уровне процесса во Вводе IP, если вы используете NAT.

Состояние нехватки памяти или поддержанная высокая загрузка ЦП (100 процентов) в Interrupt Levels могут заставить маршрутизатор Cisco IOS® перезагружаться. Перезагрузка, вызываемая процессом, который ведёт себя неправильно из-за чрезвычайных условий.

Если вы не подозреваете, что устройства на Вашем узле заражены, или являются целью червя "Code Red", то см. секцию Дополнительная информация, в разделе дополнительные адреса о том, как устранить любые неполадки, обнаруженные вами.

Определите зараженное устройство

Используйте коммутацию потоков для определения IP - адреса источника устройства, на которое влияют. Настройте ip route-cache flow на всех интерфейсах для записи всех потоков, коммутированных маршрутизатором.

После нескольких минут выполните команду show ip cache flow для просмотра зарегистрированных записей. Во время начальной фазы заражения червя "Code Red" червь пытается реплицировать себя. Когда червь отправляет запросы HT к случайным IP-адресам, репликация происходит. Поэтому необходимо искать записи потока кэш-памяти с портом назначения 80 (HT., 0050 в hex).

Команда show ip cache flow | include 0050 отображает все записи в кэше с портом TCP 80 (0050 в 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
```

При обнаружении аномально высокого количества записей с тем же IP - адресом источника, Address1 IP случайного получателя, DstP = 0050 (HTTP) и PR = 06 (TCP), вы, вероятно, определили местоположение зараженного устройства. В этом примере выходных данных IP - адрес источника 193.23.45.35 и прибывает из VLAN1.

[1]Another версия червя "Code Red", вызванного "Code Red II", не выбирает полностью IP-адрес случайного получателя. Вместо этого "Code Red II" поддерживает часть сети IP-адреса и выбирает случайную часть, относящуюся к хосту IP-адреса для распространения. Это позволяет червю распространяться быстрее в той же сети.

"Code Red II" использования эти сети и маски:

```
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)
```

Целевые IP - адреса, которые исключены, равняются 127. X. X. X и 224. X. X. X, и никакой октет позволен быть 0 или 255. Кроме того, хост не пытается повторно заразить себя.

Для получения дополнительной информации обратитесь к Code Red (II).

Иногда, вы не можете выполнить netflow для обнаружения попытки инвазии "Code Red". Это может быть то, потому что вы выполняете версию кода, которая не поддерживает netflow, или потому что маршрутизатор имеет недостаточную или чрезмерно фрагментированную память для включения netflow. Cisco рекомендует не включить netflow, когда существуют множественные входные интерфейсы и только один исходящий интерфейс на маршрутизаторе, потому что учет NetFlow выполнен на пути для внешнего доступа. В этом случае лучше включить учет для протокола IP на одиноком исходящем интерфейсе.

Примечание: Команда ip accounting отключает DCEF. Не включайте учет для протокола IP ни на какой платформе, где вы хотите использовать Коммутацию DCEF.

```
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
```

В выходных данных команды show ip accounting ищите адреса источника, которые пытаются передать пакеты несколько адресов назначениям. Если зараженный главный компьютер находится в фазе просмотра, он пытается установить соединения HTTP к другим маршрутизаторам. Таким образом, вы будете видеть попытки достигнуть несколько IP - адресовов. Большинство этих попыток подключения обычно отказывает. Поэтому вы видите только небольшое количество переданных пакетов, каждый с маленьким количеством байтов. В данном примере вероятно, что 20.1.145.49 и 20.1.104.194 заражены.

При выполнении Многоуровневой коммутации (MLS) на Catalyst 5000 и Коммутаторе Catalyst серии 6000 необходимо сделать другие шаги, чтобы включить учет NetFlow и разыскать инвазию. В коммутаторе Cat6000, оборудованном Функциональной Картой Многоуровневого Коммутатора (MSFC) Supervisor 1 (MSFC1) или SUP I/MSFC2, основанный на netflow MLS включен по умолчанию, но режим потока является destination-only. Поэтому IP - адрес источника не кэшируется. Можно позволить "полнопоточному" режиму разыскать зараженные главные компьютеры с помощью команды set mls flow full на супервизоре.

Для Гибридного режима используйте **команду 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.
```

Для Собственного режима IOS используйте команду mls flow ip full:

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

При включении "полнопоточного" режима предупреждение отображено для указания на существенное увеличение в записях MLS. Если ваша сеть уже наполнена червем "Code Red", влияние увеличенных записей MLS допустимо для небольшого времени. Червь заставляет ваши записи MLS быть чрезмерными и повышаться.

Для просмотра собранных сведений используйте эти команды:

Для Гибридного режима используйте **команду 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.
```

Для Собственного режима IOS используйте **команду mls flow ip full**:

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

При включении "полнопоточного" режима предупреждение отображено для указания на существенное увеличение в записях MLS. Если ваша сеть уже наполнена червем "Code Red", влияние увеличенных записей MLS допустимо для небольшого времени. Червь заставляет ваши записи MLS быть чрезмерными и повышаться.

Для просмотра собранных сведений используйте эти команды:

Для Гибридного режима используйте show mls ent команда:

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

Примечание: Все эти поля заполнены в том, когда они находятся в "полнопоточном" режиме.

Для Собственного режима IOS используйте **команду show mls ip**:

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

При определении IP - адреса источника и порта назначения, вовлеченного в атаку вы можете set MLS назад к режиму "destination-only".

Поскольку Гибридный режим использует команду destination set mls flow:

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

Для Собственного режима IOS используйте **команду destination ip** mls flow:

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

Супервизор (SUP), комбинация II/MSFC2 защищена от атаки, потому что коммутация CEF выполнена в аппаратных средствах, и статистика сетевых потоков поддержана. Так, даже во время атаки "Code Red" при включении полнопоточного режима маршрутизатор не затопляется из-за более быстрого механизма переключения. Команды, чтобы включить полнопоточный режим и отобразить статистику являются тем же и на SUP I/MFSC1 и на SUP II/MSFC2.

Способы предотвращения неполадок

Используйте способы, перечисленные в этом разделе для уменьшения влияния червя "Code Red" на маршрутизаторе.

Блочный трафик к порту 80

Если это выполнимо в вашей сети, самый легкий способ предотвратить атаку "Code Red" состоит в том, чтобы заблокировать весь трафик к порту 80, который является стандартным портом для WWW. Создайте access-list, чтобы запретить пакеты IP, предназначенные к порту 80 и применить его входящий на интерфейс, который стоит перед зараженным источником.

Уменьшите использование памяти для ввода ARP

Ввод ARP израсходовал огромное количество памяти, когда статический маршрут указывает к поддерживающему широковещательные сообщение интерфейс, как это:

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

Каждый пакет для маршрута по умолчанию передан к VLAN3. Однако нет никакого IP-адреса следующего перехода, заданного, и таким образом, маршрутизатор передает запрос ARP за IP - адресом назначения. Маршрутизатор следующего перехода для того назначения отвечает с его собственным MAC-адресом, пока не отключен Прокси - протокол преобразования адресов. Ответ от маршрутизатора создает дополнительную запись в таблице ARP, где IP - адрес назначения пакета сопоставлен с MAC-адресом следующего перехода. Червь "Code Red" передает пакеты случайным IP-адресам, который добавляет новую Запись ARP для каждого адреса случайного получателя. Каждая новая Запись ARP использует все больше памяти при процессе Ввода ARP.

Не создавайте статический маршрут по умолчанию к интерфейсу, особенно если интерфейс передан (Ethernet/Fast Ethernet/GE/SMDS) или многоточечный (Frame Relay / ATM). Любой статический маршрут по умолчанию должен указать к IP-адресу маршрутизатора следующего перехода. После изменения маршрута по умолчанию для обращения к IP-адресу следующего перехода, используйте **команду clear arp-cache** для очистки всех Записей ARP. Эта команда решает проблему загруженности памяти.

Используйте метод коммутации CEF

Для понижения загрузки ЦПУ на маршрутизатор IOS изменитесь от Быстрой/оптимальной/NetFlow коммутации до коммутации CEF. Существует несколько предупреждений включить CEF. Следующий раздел обсуждает различие между коммутацией CEF и быстрой коммутацией, и объясняет результаты при включении CEF.

Сравнение технологии Cisco Express Forwarding и технологии быстрой коммутации Fast Channel

Позвольте CEF облегчить увеличение трафика, вызванное червем "Code Red". Версии Программного обеспечения Cisco IOS 11.1 () CC, 12.0, и более поздний CEF поддержки на платформах Cisco 7200/7500/GSR. Поддержка CEF на других платформах доступна в программном обеспечении Cisco IOS версии 12.0 или позже. Можно заняться расследованиями далее с Советником по программному обеспечению.

Иногда, вы не можете включить CEF на всех маршрутизаторах к одной из этих причин:

- Недостаточная память
- Неподдерживаемые архитектуры платформы
- Неподдерживаемые инкапсуляции интерфейса

Поведение и последствия быстрого коммутирования

Вот результаты при использовании быстрой коммутации:

- Трафик, который ведут кэшем — кэш пуст до пакетов маршрутизаторов-коммутаторов и заполняет кэш.
- Первый пакет является коммутированным процессом — первый пакет является процессной коммутацией, потому что кэш первоначально пуст.
- Гранулированный кэш — кэш создан при глубине детализации самой определенной части записи Routing Information Base (RIB) крупной сети. Если RIB имеет / 24 для крупной сети 131.108.0.0, кэш создан с / 24 для этой крупной сети.
- /32 кэш используется —/32, кэш используется для балансировки загрузки для каждого назначения. Когда загрузка балансов кэша, кэш создан с / 32 для той крупной сети.**Примечание:** Из-за двух последних проблем кэш может достичь очень больших размеров и занять всю память.
- При кэшировании в границах крупной сети — С маршрутом по умолчанию, кэширование выполнено в границах крупной сети.
- Устаревание кэша — устаревание кэша выполняется каждую минуту и проверяет 1/20-й (5 процентов) кэша для неиспользуемых записей под обычными состояниями памяти, и 1/4-й (25 процентов) кэша в состоянии нехватки памяти (200k).

Для изменения вышеупомянутых значений используйте **команду ip cache-ager-interval X Y Z**, где:

- X <0-2147483> кол-во секунд между выполнениями ager. По умолчанию = 60 секунд.
- Y <2-50> 1 / (Y+1) кэша для устаревания на выполненный (нижняя область памяти). По умолчанию = 4.
- Z <3-100> 1 / (Z+1) кэша для устаревания на (обычный) выполненный. По умолчанию = 20.

Вот пример конфигурации, который использует **ip cache-ager 60 5 25**.

```
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
```

На основе значения вашего устаревания кэша, некоторого процента от вашего возраста записей в кэше из вашей таблицы быстрого кэша. Когда возраст записей быстро, больший процент от возрастов таблицы быстрого кэша и таблица кэш-памяти становятся меньшими.

В результате использование памяти на маршрутизаторе уменьшает. Недостаток - то, что трафик продолжает течь для записей, которые были в возрасте из таблицы кэш-памяти. Начальные пакеты являются процессной коммутацией, которая вызывает короткий скачок в потреблении ЦПУ во **Вводе IP**, пока новая запись в кэше не создана для потока.

От Cisco IOS Software Release 10.3 (8), 11.0 (3) и позже, IP - кэш ager обрабатывается по-другому, как объяснено здесь:

- **Ip cache-ager-interval** и **команды ip cache-invalidate-delay** доступны, только если **команда service internal** определена в конфигурации.
- Если период между ager выполнениями аннулирования установлен в 0, процесс устаревания отключен полностью.
- Время выражено в секундах.

Примечание: Когда вы выполняете эти команды, загрузку ЦПУ увеличений маршрутизатора. Используйте эти команды только при необходимости.

```
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
```

Преимущества CEF

- Таблица FIB строится на основе таблицы маршрутизации, поэтому информация о пересылке создается еще перед пересылкой первого пакета. FIB также содержит /32 записи для непосредственно связанных хостов LAN.
- Таблица смежности содержит данные перезаписи уровня 2 для следующих узлов и хостов, подключенных напрямую (запись ARP создает смежность CEF).
- CEF для бросков CPU не имеет понятия устаревания кеш-памяти. Если запись таблицы маршрутизации удалена, запись FIB удалена.

Внимание. : Снова, маршрут по умолчанию, который указывает к широковещанию или многоточечному интерфейсу, означает, что маршрутизатор передает запросы ARP за каждым новым назначением. Запросы ARP от маршрутизатора потенциально создают огромную таблицу соседей, пока маршрутизатор не исчерпывает память. Если сбои CEF для выделения CEF/DCEF памяти отключают себя. Необходимо будет вручную включить CEF/DCEF снова.

Образец выходных данных: CEF

Вот некоторый пример выходных данных **команды show ip cef summary**, которая показывает использование памяти. Эти выходные данные являются снимком от сервера маршрутов Cisco 7200 с программным обеспечением Cisco IOS версии 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
```

Что следует учесть

Когда количество потоков является большим, CEF, как правило, использует меньше памяти, чем быстрая коммутация. Если память уже использована кэшем быстрой коммутации, необходимо очистить кэш ARP (посредством **команды clear ip arp**) перед включением CEF.

Примечание: При очистке кэша скачок вызван в загрузке ЦПУ маршрутизатора.

Часто задаваемые вопросы "Code Red" и их ответы

Вопрос. . Я использую NAT и испытываю 100 процентов использования CPU во Вводе IP. Когда я выполняю ЦПУ show proc, моя загрузка ЦПУ высока в Interrupt Levels - 100/99 или 99/98. Это может быть отнесено к "Code Red"?

O. Там недавно исправлен ошибка Cisco NAT (CSCdu63623 (только зарегистрированные клиенты)), который включает масштабируемость. Когда существуют десятки тысяч потоков NAT (на основе типа платформы), дефект вызывает 100 процентов использования CPU при процессе или Interrupt Levels.

Чтобы определить, является ли этот дефект причиной, выполните **команду show align** и проверьте, стоит ли маршрутизатор перед ошибками выравнивания. Если вы действительно видите ошибки выравнивания или ложные доступы к памяти, выполняете **команду show align** пару раз и видите, повышаются ли ошибки. Если количество ошибок повышается, ошибки выравнивания могут быть причиной высокой загрузки ЦП в Interrupt Levels, и не ошибкой Cisco CSCdu63623 (только зарегистрированные клиенты). Для получения дополнительной информации обратитесь к Устранению проблем Подложных доступов и Ошибок выравнивания.

Команда **show ip nat translation** отображает количество активных трансляций. Точка краха для процессора класса NPE-300 является приблизительно 20,000 - 40,000 трансляций. Этот номер варьируется на основе платформы.

Эта проблема разрушения наблюдалась ранее несколькими клиентами, но после "Code Red", больше клиентов испытало эту проблему. Единственный обходной путь должен выполнить NAT (вместо PAT), так, чтобы было меньше активных трансляций. Если у вас есть 7200, используйте NSE-1 и понизьте значения таймаута NAT.

Вопрос. . Я запустил IRB и столкнулся с высокой загрузкой CPU процессом

HyBridge Input. Почему это происходит? Это связано с «Code Red»?

O. Процесс HyBridge Input обрабатывает любые пакеты, которые не могут быть выполнены быструю коммутацию процессом IRB. Неспособность процесса IRB выполнить быструю коммутацию пакет может состоять в том потому что:

- Пакет является транслируемым пакетом.
- Пакет является пакетом групповой адресации.
- Назначение неизвестно, и ARP должен быть инициирован.
- Существуют BPDU связующего дерева.

Если существуют тысячи интерфейсов точка-точка в той же группе мостов, процесс HyBridge Input встречается с проблемами. Процесс HyBridge Input также встречается с проблемами (но до меньшей степени), если существуют тысячи VS в том же многоточечном интерфейсе.

Возможные причины неполадок с IRB? Предположите, что устройство, зараженное "Code Red", просматривает IP-адреса.

- Маршрутизатор должен передать запрос ARP за каждым IP - адресом назначения. Лавинная рассылка запросов ARP приводит на каждом VC к группе мостов для каждого адреса, который просмотрен. Обычный процесс ARP не вызывает проблему ЦПУ. Однако, если существует Запись ARP без записи моста, пакеты потоков маршрутизатора, предназначенные для адресов, для которых уже существуют Записи ARP. Это может привести к высокой загрузке CPU, так как трафик переключается процессами. Для предотвращения проблемы увеличьте время тренировки моста (по умолчанию 300 секунд или 5 минут), чтобы совпасть или превысить тайм-аут ARP (по умолчанию 4 часа) так, чтобы синхронизировались эти два таймера.
- Адрес, который конечный хост пытается заразить, является широковещательным адресом. Маршрутизатор создает эквивалент широковещания подсети, который процесс HyBridge Input должен воспроизвести. Если команда **no ip directed-broadcast** настроена, это не происходит. От программного обеспечения Cisco IOS версии 12.0 **команда ip directed-broadcast** отключена по умолчанию, который заставляет все НАПРАВЛЕННЫЕ ШИРОКОВЕЩАТЕЛЬНЫЕ IP - РАССЫЛКИ быть отброшенными.
- Вот примечание стороны, не связанное друг с другом к "Code Red" и отнесенное к архитектурам IRB:Групповая адресация уровня 2 и транслируемые пакеты должны быть реплицированы. Поэтому проблема с серверами IPX, которые работают на широковещательном сегменте, может перевести ссылку в нерабочее состояние. Можно использовать абонентскую политику для предотвращения проблемы. Для получения дополнительной информации обратитесь к x Digital Subscriber Line (xDSL) Bridge Support. Необходимо также рассмотреть access-lists моста, которые ограничивают тип трафика, позволенный проходить через маршрутизатор.
- Для облегчения этой проблемы IRB можно использовать группы множественных мостов и гарантировать, что существует однозначное сопоставление для BVI, подчиненных интерфейсов и VC.
- RBE превосходит IRB потому что, предоставляет стек моста в целом. Можно мигрировать на RBE от IRB. Эти ошибки Cisco вдохновляют такую миграцию:CSCdr11146 (только зарегистрированные клиенты)CSCdp18572 (только зарегистрированные клиенты)CSCds40806 (только зарегистрированные клиенты)

Вопрос. . Моя загрузка ЦПУ высока в Interrupt Levels, и я получаю сбросы, если я пробую show log. Скорость трафика несколько выше стандартной. Какова причина для этого?

O. Вот пример выходных данных **команды 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
```

Проверьте, регистрируете ли вы к консоли. Если так, проверьте, существуют ли запросы HTTP трафика. Затем, проверьте, существует ли какой-либо access-lists с регистрационными ключевыми словами или отладками, которые наблюдают определенного Ip flow. Если сбросы повышаются, это может быть, потому что консоль, обычно 9600 устройств со скоростью передачи в бодах, неспособна обработать полученное количество данных. В этом сценарии маршрутизатор отключает прерывания и действительно только обрабатывает консольные сообщения. Решение состоит в том, чтобы отключить вход через консоль или удалить любой тип регистрации, вы выполняете.

Вопрос. . Я вижу многочисленные попытки соединения HTTP на своем маршрутизаторе IOS, который выполняет ip http server. Это связано с червем "Code Red"?

O. "Code Red" может быть причиной здесь. Cisco рекомендует отключить **команду ip http server** на маршрутизаторе IOS так, чтобы это не имело дело с многочисленными попытками подключения от зараженных главных компьютеров.

Обходные пути

Существуют различные обходные пути, которые обсуждены в Информационных сообщениях, которые Обсуждают раздел Червя "Code Red". См. информационные сообщения для обходных путей.

Другой метод для блокирования "Code Red" собирает червей при Uses Network-Based Application Recognition точек входа в сеть (NBAR) и Списки контроля доступа (ACL) в рамках программного обеспечения IOS на маршрутизаторах Cisco. Используйте этот метод в сочетании с рекомендуемыми пакетами исправлений для серверов IIS от Microsoft. Для получения дополнительной информации об этом методе обратитесь к Использованию NBAR и ACL для Блокирования Червя "Code Red" в Точках входа в сеть.

Дополнительные сведения

- Устранение неполадок, связанных с памятью
- Устранение неисправностей при буферных утечках
- Решение проблемы высокой загрузки CPU на маршрутизаторах Cisco
- Устранение неполадок при сбое маршрутизатора
- Технические примечания по поиску и устранению проблем - маршрутизаторы
- Устранение неполадок с маршрутизатором
- Cisco Systems – техническая поддержка и документация