# Рекомендация Cisco по вопросам безопасности: Уязвимость к специально созданным параметрам IP

---

**Идентификатор рекомендации: cisco-sa-20070124-crafted-ip-option**

**http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml**

## Редакция 1.3

**Последнее обновление 2 февраля 2007 г. 21:00 UTC (GMT)**

**Публичный выпуск: 24 января 2007 г. 16:00 UTC (GMT)**

---

**Пожалуйста, оставьте отзыв на этот документ.**

---

## Содержание



---

## Обзор

Маршрутизаторы и коммутаторы Cisco под управлением ПО Cisco IOS® или Cisco IOS XR могут быть уязвимы к атаке DOS (Denial of service) на основе специально созданного параметра IP. Эту уязвимость можно использовать удаленно. Уязвимость дает злоумышленнику потенциальную возможность запуска произвольного кода. Злоумышленник может воспользоваться уязвимостью, если устройство обработает пакет ICMP, PIMv2, PGM или URD с определенным, специально созданным параметром IP в заголовке IP. Другие протоколы IP не подвержены влиянию этой проблемы.

Cisco предоставляет пострадавшим заказчикам бесплатное программное обеспечение для решения этой проблемы.

Существуют временные решения, которые позволяют снизить воздействие проблемы.

Уязвимость была обнаружена во время внутреннего тестирования.

Эта рекомендация доступна по адресу http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml.

## Продукты, подверженные влиянию проблемы

### Уязвимые продукты

Эта проблема затрагивает все устройства Cisco под управлением ПО Cisco IOS или Cisco IOS XR, настроенные на обработку пакетов IPv4. Устройства, которые работают только с версией IPv6 не подвержены влиянию проблемы.

Уязвимость присутствует во всех неисправленных версиях ПО Cisco IOS, включая 9.x, 10.x, 11.x и 12.x.

Уязвимость присутствует во всех неисправленных версиях ПО Cisco IOS XR включая 2.0.X, 3.0.X, and 3.2.X.

Все версии Cisco IOS или Cisco IOS XR, предшествующие версиям, указанным в таблице исправленного программного обеспечения, могут быть подвержены влиянию этой уязвимостью.

Чтобы определить, какое программное обеспечение работает на продукте Cisco, войдите в систему устройства и выполните команду **show version**, чтобы отобразить системный баннер. ПО Cisco IOS определяется как "Internetwork Operating System Software" или просто "IOS". В следующей строке выходных данных будет отображаться имя образа в скобках, слово "Version" и имя версии IOS. ПО Cisco IOS XR определяется как "Cisco IOS XR Software", затем идет слово "Version" и номер версии. Другие устройства Cisco не отреагируют на команду **show version** или вернут другие выходные данные.

В этом примере идентифицируется продукт Cisco под управлением версии Cisco IOS 12.2(14)S16 с установленным образом C7200-IS-M:

```
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-IS-M), Version 12.2(14)S16, RELEASE SOFTWARE (fc1)
```

Метка последовательности версий — "12.2".

В примере ниже рассматривается продукт Cisco под управлением версии IOS 12.3(7)T12 с образом C7200-IK9S-M:

```
Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(7)T12, RELEASE SOFTWARE (fc1)
```

Дополнительные сведения о баннерах Cisco IOS доступны по адресу http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml#3.

ПО IOS XR входит в семейство программного обеспечения Cisco IOS, использующее распределенную инфраструктуру ОС на основе микроядер. Cisco IOS XR работает только на Cisco Carrier Routing System 1 (CRS-1) и маршрутизаторах серии Cisco XR 12000.

Дополнительные сведения о ПО Cisco IOS XR доступны по адресу http://www.cisco.com/en/US/products/ps5845/index.html

В примерах ниже приводятся неполные выходные данные команды **show version**, идентифицирующей продукт Cisco под управлением Cisco IOS XR 3.3.0:

```
RP/0/RP0/CPU0:router#show version
Cisco IOS XR Software, Version 3.3.0
Copyright (c) 2006 by Cisco Systems, Inc.
ROM: System Bootstrap, Version 1.32(20050525:193559) [CRS-1 ROMMON]
```

### Продукты, гарантированно не подверженные влиянию уязвимости

Устройства Cisco, которые не работают под управлением ПО Cisco IOS или Cisco IOS XR, не подвержены действию проблемы. ПО CatOS не подвержено влиянию уязвимости.

Насколько нам известно, другие продукты Cisco не подвержены влиянию проблемы.

## Подробные сведения

Злоумышленник сможет воспользоваться этой уязвимостью, если устройство, подверженное влиянию проблемы, обработает пакет, соответствующий *всем трем* указанным ниже условиям.

| |
|---|
| **1. Пакет содержит специально созданный параметр IP.** |
| ***И*** |
| **2. Пакет принадлежит одному из следующих протоколов:** |
| • ICMP — эхо-запрос (тип 8) — "ping" |
| • ICMP — временная метка (тип 13) |
| • ICMP — информационный запрос (тип 15) |
| • ICMP — запрос маски адреса (тип 17) |
| • PIMv2 — протокол IP 103 |
| • PGM — протокол IP 113 |
| • URD — TCP-порт 465 |
| ***И*** |
| **3. Пакет должен быть отправлен по физическому или виртуальному адресу IPv4, настроенному на уязвимом устройстве.** |

Другие типы сообщений ICMP не подвержены влиянию этой проблемы.

Другие протоколы IP не подвержены влиянию этой проблемы.

Другие службы TCP не подвержены влиянию этой проблемы.

Пакет может быть отправлен как из локальной, так и из удаленной сети.

IP-адрес источника пакета может быть подделанным или подлинным.

Пакеты, который проходят через устройство как транзитные (т. е. отправленные не по одному из IP-адресов устройства) не активируют уязвимость и устройство не подвергается действию проблемы.

Эта уязвимость задокументирована в следующих документах Bug ID:

- Cisco Bug ID CSCec71950 (только для зарегистрированных заказчиков) для Cisco IOS
- Cisco Bug ID CSCeh52410 (только для зарегистрированных заказчиков) для Cisco IOS XR

### Cisco IOS

Специально созданный IP-пакет, направленный по одному из адресов уязвимого устройства под управлением Cisco IOS может привести к перезагрузке устройства или сделать возможным выполнение произвольного кода.

### Cisco IOS XR

Специально созданный IP-пакет, направленный по одному из адресов уязвимого устройства под управлением Cisco IOS XR, может привести к перезапуску процесса ipv4_io или сделать возможным выполнение произвольного кода. Узлы CRS-1 под управлением процесса ipv4_io включают процессоры маршрутизации (RP), распределенные процессоры маршрутизации (DRP), платы модульных служб (MSC) и линейные платы XR 12000. Пока процесс ipv4_io перезапускается, весь ICMP-трафик, предназначенный для устройства, и исключения будут отброшены. Примеры исключений — пакеты с данными в заголовке IP, которые требуют дальнейшей обработки, например параметры IP, значения Time-to-Live, равные 0 или 1 и сигналы Keepalive второго уровня. Трафик CLNS к узлу или линейной плате не подвержен влиянию этой проблемы. Если процесс ipv4_io перезапускается несколько раз подряд, узел CRS-1 или линейная плата XR 12000 могут перезагрузиться, что приведет к образованию состояния Denial of Service (DoS) для транзитного трафика, коммутируемого этим узлом или линейной платой.

### Устройства, настроенные для типов сообщений ICMP

#### ICMP тип 8

По умолчанию устройства под управлением всех версий Cisco IOS и Cisco IOS XR обрабатывают пакеты эхо-запроса ICMP (тип 8). Это нельзя изменить.

#### ICMP тип 13

По умолчанию устройства под управлением всех версий Cisco IOS обрабатывают пакеты временных меток ICMP (тип 13). Это нельзя изменить.

По умолчанию устройства под управлением всех версий Cisco IOS XR НЕ обрабатывают пакеты временных меток ICMP (тип 13). Это нельзя изменить.

#### ICMP тип 15

С появлением улучшения CSCdz50424, маршрутизаторы НЕ обрабатывают пакеты информационных запросов ICMP (тип 15) по умолчанию. Версии Cisco IOS, включающие CSCdz50424: 12.3, 12.3T, 12.4, 12.4T, 12.0S, 12.2S и выше. См. полные сведения о версии в документе CSCdz50424 (только для зарегистрированных заказчиков).

Маршрутизатор под управлением версии Cisco IOS, включающей CSCdz50424, который настроен на обработку пакетов информационных запросов ICMP будет иметь инструкцию **ip information-reply** в конфигурации интерфейса. Наличие этой инструкции можно проверить с помощью команды **show running-config**, как показано в примерах ниже:

```
router#show running-config | include information-reply
 ip information-reply
```

или

```
router#show running-config

interface FastEthernet0/0
 ip address 192.0.2.1 255.255.255.0
 ip information-reply
```

По умолчанию устройства под управлением всех остальных версий Cisco IOS будут обрабатывать пакеты информационных запросов ICMP (тип 15). Это нельзя изменить. Поскольку это — режим работы по умолчанию, инструкция **ip information-reply** не будет отображаться в конфигурации устройства.

По умолчанию устройства под управлением всех версий Cisco IOS XR НЕ обрабатывают пакеты информационных запросов ICMP (тип 15). Это нельзя изменить.

**ICMP тип 17**

Начиная с версии Cisco IOS 10.0, по умолчанию устройства НЕ обрабатывают пакеты запросов маски адреса ICMP (тип 17). Маршрутизатор, который настроен на обработку пакетов запроса маски адреса ICMP будет иметь инструкцию **ip mask-reply** в конфигурации интерфейса. Наличие этой инструкции можно проверить с помощью команды **show running-config**, как показано в примерах ниже:

```
router#show running-config | include mask-reply
ip mask-reply
```

или

```
router#show running-config

interface FastEthernet0/0
ip address 192.0.2.1 255.255.255.0
ip mask-reply
```

По умолчанию устройства под управлением всех версий Cisco IOS XR НЕ обрабатывают пакеты запроса маски адреса ICMP (тип 17). Маршрутизатор, который настроен на обработку пакетов запросов маски адреса ICMP будет иметь инструкцию **ipv4 mask-reply** в конфигурации интерфейса. Наличие этой инструкции можно проверить с помощью команды **show running-config**, как показано в примерах ниже:

```
RP/0/RP0/CPU0:router#show running-config | include mask-reply
Building configuration...
ipv4 mask-reply
```

или

```
RP/0/RP0/CPU0:router#show running-config
interface POS0/1/3/0
ipv4 address 192.0.2.1 255.255.255.252
ipv4 mask-reply
```

### Устройства, настроенные на использование PIMv2 (Protocol Independent Multicast Version 2)

#### Cisco IOS

Маршрутизатор под управлением Cisco IOS, настроенный на обработку пакетов PIMv2, будет иметь инструкцию, начинающуюся с **ip pim** в конфигурации интерфейса. Наличие этой инструкции можно проверить с помощью команды **show running-config**, как показано в примерах ниже:

```
router#show running-config | include ip pim
ip pim sparse-mode
```

или

```
router#show running-config

interface FastEthernet0/0
ip address 192.0.2.1 255.255.255.0
ip pim sparse-dense-mode
```

Кроме того, команда **show ip pim interface** позволяет определить, настроен ли маршрутизатор на обработку пакетов PIMv2, как показано в примере ниже:

```
router#show ip pim interface
Address         Interface           Ver/    Nbr     Query  DR      DR
                Mode    Count   Intvl  Prior
192.0.2.1       FastEthernet0/0     v1/S    0       30     1       0.0.0.0
192.168.1.1     FastEthernet1/0     v2/SD   0       30     1       0.0.0.0
```

Интерфейсы, обрабатывающие PIMv2, будут отображать параметр "v2/" в столбце **Ver/Mode**. Интерфейсы, на которых протокол PIM не настроен, не будут отображаться в выходных данных команды.

PIMv2 — это версия PIM по умолчанию. Маршрутизаторы, настроенные на обработку только сообщений PIMv1, не подвержены уязвимости PIMv2. Маршрутизаторы, на которых протокол PIM не настроен, не подвержены влиянию этой проблемы уязвимостью PIMv2. Протокол PIM по умолчанию отключен.

Дополнительные сведения о протоколе PIM доступны по адресу http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca794.html.

#### Cisco IOS XR

Чтобы определить, настроен ли маршрутизатор под управлением Cisco IOS XR на обработку пакетов PIMv2, можно использовать команду **show pim interface**. См. пример ниже:

```
RP/0/0/CPU0:router#show pim interface
Address                 Interface           PIM  Nbr   Hello  DR    DR
                                                 Count Intvl  Prior
192.168.1.1             Loopback0           on   1     30     1     this system
192.168.2.1             MgmtEth0/0/CPU0/0   off  0     30     1     not elected
192.168.3.1             Loopback1           on   1     30     1     this system
192.168.4.1             Loopback3           on   1     30     1     this system
192.168.5.1             POS0/4/0/0          on   1     30     1     this system
192.0.2.1               POS0/4/0/1          on   1     30     1     this system
```

Интерфейсы, обрабатывающие PIMv2, будут отображать параметр **on** в столбце **PIM**. Интерфейсы, в которых протокол PIM не

настроен, будут отображать параметр "off" в столбце **PIM**.

Cisco IOS XR не поддерживает PIMv1. По умолчанию протокол PIM отключен в программном обеспечении Cisco IOS XR.

Дополнительные сведения об использовании протокола PIM в ПО Cisco IOS XR доступны по адресу http://www.cisco.com/en/US/products/ps5845/products_configuration_guide_chapter09186a008069a8a2.html.

### Устройства, настроенные на использование протокола PGM (Pragmatic General Multicast)

Маршрутизаторы, настроенные на обработку пакетов PGM, будут иметь инструкцию **ip pgm router** в конфигурации интерфейса. Наличие этой инструкции можно проверить с помощью команды **show running-config**, как показано в примерах ниже:

```
router#show running-config | include ip pgm
ip pgm router
```

или

```
router#show running-config

interface FastEthernet1/0
 ip address 192.0.2.1 255.255.255.0
 ip pim sparse-dense-mode
 ip pgm router
```

или

```
router#show running-config

interface FastEthernet1/0
ip address 192.0.2.1 255.255.255.0
ip pgm router
```

Маршрутизаторы, на которых протокол PGM не настроен, не будут подвержены влиянию уязвимости PGM. Протокол PGM по умолчанию отключен.

Дополнительные сведения о протоколе PGM доступны по адресу http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca798.html.

ПО Cisco IOS XR не поддерживает протокол PGM и не подвержено влиянию пакетов PGM, которые используют эту уязвимость.

### Устройства, настроенные на использование протокола URD (URL Rendezvous Directory)

Маршрутизаторы, настроенные на обработку пакетов PGM, будут иметь инструкцию **ip urd** *или* **ip urd proxy** в конфигурации интерфейса. Наличие этих инструкций можно проверить с помощью команды **show running-config**, как показано в примерах ниже:

```
router#show running-config | include ip urd
ip urd
```

или

```
router#show running-config | include ip urd
ip urd proxy
```

или

```
router#show running-config

interface FastEthernet1/0
 ip address 192.0.2.1 255.255.255.0
 ip pim sparse-mode
 ip urd
```

или

```
router#show running-config

interface FastEthernet1/0
 ip address 192.0.2.1 255.255.255.0
 ip pim sparse-dense-mode
 ip urd proxy
```

или

```
router#show running-config

interface FastEthernet1/0
ip address 192.0.2.1 255.255.255.0
ip urd
```

Маршрутизаторы, на которых протокол URD не настроен, не будут подвержены влиянию уязвимости URD. Протокол URD по умолчанию отключен.

Дополнительные сведения о протоколе URD доступны по адресу http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca795.html.

ПО Cisco IOS XR не поддерживает протокол URD и не подвержено влиянию пакетов URD, которые используют эту уязвимость.

## Сведения о показателях уязвимости

В этой рекомендации Cisco представляет показатели уязвимости, основанные на Common Vulnerability Scoring System (CVSS). Cisco предоставляет временные и базовые показатели. Затем заказчики могут рассчитать показатели для своих сред, чтобы определить влияние уязвимости на отдельные сети.

Cisco PSIRT установит нормальное смещение для всех случаев. Заказчикам рекомендуется применять параметр смещения при определении влияния той или иной уязвимости на среду.

CVSS — это стандартизированный метод расчета показателей уязвимости, который позволяет измерить степень воздействия уязвимости, а также определить срочность и приоритетность ответа.

Cisco предлагает ознакомится с ответами на дополнительные вопросы по CVSS по адресу http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html.

Cisco предоставляет калькулятор CVSS, который позволяет рассчитать влияние уязвимости на отдельные сети. Его можно найти по адресу http://intellishield.cisco.com/security/alertmanager/cvss.

| **CSCec71950 (только для зарегистрированных заказчиков) — специально созданный параметр IP может вызвать состояние DoS или привести к выполнению кода**<br><br>**Расчет показателя CSCec71950 для среды** |
|---|

Базовый показатель CVSS — **10**

| Вектор доступа | Сложность доступа | Аутентификация | Влияние на конфиденциальность | Влияние на целостность | Влияние на доступность | Смещение для влияния |
|---|---|---|---|---|---|---|
| Удаленный | Низкое | Не требуется | Полное | Полное | Полное | Нормальный |

Временной показатель CVSS — **8,3**

| Возможность использования уязвимости | Уровень действий по решению проблемы | Достоверность отчета |
|---|---|---|
| Функциональна | Официальное исправление | Подтверждена |

| **CSCeh52410 (только для зарегистрированных заказчиков) — специально созданный параметр IP может вызвать состояние DoS для процесса ipv4-io или привести к выполнению кода**<br><br>**Расчет показателя CSCeh52410 для среды** |
|---|

Базовый показатель CVSS — **10**

| Вектор доступа | Сложность доступа | Аутентификация | Влияние на конфиденциальность | Влияние на целостность | Влияние на доступность | Смещение для влияния |
|---|---|---|---|---|---|---|
| Удаленное | Низкое | Не требуется | Полное | Полное | Полное | Нормальное |

Временной показатель CVSS — **8,3**

| Возможность использования уязвимости | Уровень действий по решению проблемы | Достоверность отчета |
|---|---|---|
| Функциональна | Официальное исправление | Подтверждена |

## Влияние

### Cisco IOS

Успешное использование уязвимости Cisco IOS может привести к перезагрузке устройства или выполнению произвольного кода. Повторное использование уязвимости может стать причиной непрерывной DoS-атаки.

### Cisco IOS XR

Успешное использование уязвимости на Cisco IOS XR может привести к перезапуску процесса ipv4_io или выполнению произвольного кода. Повторное использование уязвимости может стать причиной перезагрузки узла CRS-1 или линейной платы XR 12000, а также привести к непрерывной DoS-атаке.

## Версии ПО и исправления

Рассматривая обновления программного обеспечения, ознакомьтесь с документом по адресу http://www.cisco.com/go/psirt и всеми последующими рекомендациями, чтобы определить потенциальную уязвимость обновленной среды.

Во всех случаях заказчикам следует проявить осторожность и убедиться, что устройства имеют достаточно памяти для обновления и что текущие аппаратные и программные конфигурации будут поддерживаться новой версией. Если вы не уверены в этой информации, обратитесь в центр технической поддержки Cisco ("TAC") или к поставщику услуг по техническому обслуживанию, с которым у вас подписан контракт.

Каждая строка таблицы Cisco IOS (см. ниже) описывает последовательность версий и платформы или продукты, для которых она предназначена. Если та или иная последовательность версий уязвима, самые ранние версии ("Первая исправленная версия") и ожидаемая дата выхода этих версий перечислены в столбцах "Повторная сборка" и "Обслуживание". Устройство, работающее под управлением версии из последовательности, предшествующей версии в данном столбце (ниже чем первая исправленная версия) будет уязвимым. Эту версию необходимо обновить как минимум до указанной версии или более поздней (более высокой или равной первой исправленной версии).

Дополнительные сведения о значении терминов "Повторная сборка" и "Обслуживание" см. по следующему URL-адресу http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml.

**Примечание:** 24 января 2007 г. опубликовано три рекомендации Cisco по вопросам безопасности IOS и одно уведомление о дефекте. В каждой рекомендации перечислены только версии, в которых исправлена проблема, описанная в этой рекомендации. Объединенная таблица программного обеспечения доступна по адресу http://www.cisco.com/warp/public/707/cisco-sa-20070124-bundle.shtml и может использоваться для подбора версии ПО, в которой устранены все уязвимости, данные о которых опубликованы 24 января 2007 г. Ссылки на рекомендации по вопросам безопасности и уведомление о дефекте:

- http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml
- http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml
- http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml
- http://www.cisco.com/warp/customer/770/fn62613.shtml

Запросы на повторную сборку, включающие изменение политики перехода на декретное время (DST), вступающее в силу в марте 2007 г. необходимо направлять в центр технической поддержки, используя эту рекомендацию для справки.

| **Основная версия** | **Доступность исправленных версий** | |
|---|---|---|
| **Уязвимые версии на базе 12.0** | **Повторная сборка** | **Обслуживание** |
| 12.0 | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0DA | Уязвима, необходима миграция на 12.2(10)DA5 или выше | |

| | | |
|---|---|---|
| 12.0DB | Уязвима, необходима миграция на 12.3(4)T13 или выше | |
| 12.0DC | Уязвима, необходима миграция на 12.3(4)T13 или выше | |
| 12.0S | 12.0(27)S3 | 12.0(28)S |
| 12.0SC | Уязвима, необходима миграция на 12.3(9a)BC или выше | |
| 12.0SL | Уязвима, необходима миграция на 12.0(28)S или выше | |
| 12.0SP | Уязвима, необходима миграция на 12.0(28)S или выше | |
| 12.0ST | Уязвима, необходима миграция на 12.0(28)S или выше | |
| 12.0SX | 12.0(25)SX11 | 12.0(30)SX |
| 12.0SY | | 12.0(27)SY |
| 12.0SZ | | 12.0(30)SZ |
| 12.0T | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0W | 12.0(28)W5(32b) | |
| 12.0WC | 12.0(5)WC15 | |
| 12.0WT | Уязвима, обратитесь в TAC | |
| 12.0XA | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XB | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XC | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XD | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XE | Уязвима, необходима миграция на 12.1(23)E или выше | |
| 12.0XF | Не уязвима | |
| 12.0XG | Уязвима, необходима миграция на 12.2(37)или выше | |

| | | |
|---|---|---|
| 12.0XH | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XI | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XJ | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XK | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XL | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XM | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XN | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XQ | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XR | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XS | Уязвима, необходима миграция на 12.1(23)E или выше | |
| 12.0XV | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.0XW | Уязвима, необходима миграция на 12.0(5)WC15 или выше | |
| **Уязвимые версии на базе 12.1** | **Повторная сборка** | **Обслуживание** |
| 12.1 | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.1AA | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.1AX | Уязвима, для c3750-ME, необходима миграция 12.2(25)EY или выше. Для c2970 и 3750, необходима миграция на 12.2(25)SE или выше. | |
| 12.1AY | Уязвима, необходима миграция на 12.1(22)EA8 | |
| 12.1AZ | Уязвима, необходима миграция на 12.1(22)EA8 | |
| 12.1CX | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.1DA | Уязвима, необходима миграция на 12.2(10)DA5 или выше | |

| | | |
|---|---|---|
| 12.1DB | Уязвима, необходима миграция на 12.3(4)T13 или выше | |
| 12.1DC | Уязвима, необходима миграция на 12.3(4)T13 или выше | |
| 12.1E | | 12.1(23)E |
| 12.1EA | 12.1(22)EA8 | |
| 12.1EB | | 12.1(23)EB |
| 12.1EC | Уязвима, необходима миграция на 12.3(9a)BC или выше | |
| 12.1EO | 12.1(19)EO6; доступна с 22.02.07 | |
| | 12.1(20)EO3 | |
| 12.1EU | Уязвима, необходима миграция на 12.2(25)EWA или выше | |
| 12.1EV | Уязвима, необходима миграция на 12.2(26)SV1 или выше | |
| 12.1EW | Уязвима, необходима миграция на 12.2(18)EW3 или выше | |
| 12.1EX | Уязвима, необходима миграция на 12.1(23)E или выше | |
| 12.1EY | Уязвима, необходима миграция на 12.1(23)E или выше | |
| 12.1EZ | Уязвима, необходима миграция на 12.1(23)E или выше | |
| 12.1T | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.1XA | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.1XB | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.1XC | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.1XD | Уязвима, необходима миграция на 12.2(37)или выше | |
| 12.1XE | Уязвима, необходима миграция на 12.1(23)E или выше | |

| | |
|---|---|
| 12.1XF | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XG | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XH | Уязвима, необходима миграция на 12.2(37)или выше |
| 12.1XI | Уязвима, необходима миграция на 12.2(37)или выше |
| 12.1XJ | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XL | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XM | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XP | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XQ | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XR | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XS | Уязвима, необходима миграция на 12.2(37)или выше |
| 12.1XT | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XU | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XV | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1XW | Уязвима, необходима миграция на 12.2(37)или выше |
| 12.1XX | Уязвима, необходима миграция на 12.2(37)или выше |
| 12.1XY | Уязвима, необходима миграция на 12.2(37)или выше |
| 12.1XZ | Уязвима, необходима миграция на 12.2(37)или выше |
| 12.1YA | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1YB | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.1YC | Уязвима, необходима миграция на 12.3(8) или выше |

| | | |
|---|---|---|
| 12.1YD | Уязвима, необходима миграция на 12.3(8) или выше | |
| 12.1YE | Уязвима, необходима миграция на 12.3(8) или выше | |
| 12.1YF | Уязвима, необходима миграция на 12.3(8) или выше | |
| 12.1YH | Уязвима, необходима миграция на 12.3(8) или выше | |
| 12.1YI | Уязвима, необходима миграция на 12.3(8) или выше | |
| 12.1YJ | Уязвима, необходима миграция на 12.1(22)EA8 | |
| **Уязвимые версии на базе 12.2** | **Повторная сборка** | **Обслуживание** |
| 12.2 | 12.2(34a) | 12.2(37) |
| 12.2B | Уязвима, необходима миграция на 12.3(4)T13 или выше | |
| 12.BC | Уязвима, необходима миграция на 12.3(9a)BC или выше | |
| 12.2BW | Уязвима, необходима миграция на 12.3(8) или выше | |
| 12.2BY | Уязвима, необходима миграция на 12.3(4)T13 или выше | |
| 12.2BZ | Уязвима, необходима миграция на 12.3(7)XI8 или выше | |
| 12.2CX | Уязвима, необходима миграция на 12.3(9a)BC или выше | |
| 12.2CY | Уязвима, необходима миграция на 12.3(9a)BC или выше | |
| 12.2CZ | Уязвима, обратитесь в TAC | |
| 12.2DA | 12.2(10)DA5 | |
| | 12.2(12)DA10 | |
| 12.2DD | Уязвима, необходима миграция на 12.3(4)T13 или выше | |
| 12.2DX | Уязвима, необходима миграция на 12.3(4)T13 или выше | |
| 12.2EU | Уязвима, необходима миграция на 12.2(25)EWA5 или | |

| | | |
|---|---|---|
| | выше | |
| 12.2EW | 12.2(18)EW3 | |
| | 12.2(20)EW4 | 12.2(25)EW |
| 12.2EWA | 12.2(20)EWA4 | 12.2(25)EWA |
| 12.2EX | | 12.2(25)EX |
| 12.2EY | Все версии 12.2EY исправлены | |
| 12.2EZ | Все версии 12.2EZ исправлены | |
| 12.2FX | Все версии 12.2FX исправлены | |
| 12.2FY | Все версии 12.2FY исправлены | |
| 12.2FZ | Все версии 12.2FZ исправлены | |
| 12.2IXA | Все версии 12.2IXA исправлены | |
| 12.2IXB | Все версии 12.2IXB исправлены | |
| 12.2IXC | Все версии 12.2IXC исправлены | |
| 12.2JA | Уязвима, необходима миграция на 12.3(8)JA или выше | |
| 12.2JK | Уязвима, необходима миграция на 12.4(4)T или выше | |
| 12.2MB | Уязвима, необходима миграция на 12.2(25)SW1 или выше | |
| 12.2MC | 12.2(15)MC2h | |
| 12.2S | | 12.2(25)S |
| 12.2SB | | 12.2(28)SB |
| 12.2SBC | Все версии 12.2SBC исправлены | |
| 12.2SE | | 12.2(25)SE |

| | | |
|---|---|---|
| 12.2SEA | Все версии 12.2SEA исправлены | |
| 12.2SEB | Все версии 12.2SEB исправлены | |
| 12.2SEC | Все версии 12.2SEC исправлены | |
| 12.2SED | Все версии 12.2SED исправлены | |
| 12.2SEE | Все версии 12.2SEE исправлены | |
| 12.2SEF | Все версии 12.2SEF исправлены | |
| 12.2SEG | Все версии 12.2SEG исправлены | |
| 12.2SG | Все версии 12.2SG исправлены | |
| 12.2SGA | Все версии 12.2SGA исправлены | |
| 12.2SO | 12.2(18)SO7 | |
| 12.2SRA | Все версии 12.2SRA исправлены | |
| 12.2SRB | Все версии 12.2SRB исправлены | |
| 12.2SU | Уязвима, необходима миграция на 12.3(14)T или выше | |
| 12.2SV | | 12.2(23)SV |
| 12.2SW | 12.2(25)SW1 | |
| 12.2SX | Уязвима, необходима миграция на 12.2(17d)SXB11a или выше | |
| 12.2SXA | Уязвима, необходима миграция на 12.2(17d)SXB11a или выше | |
| 12.2SXB | 12.2(17d)SXB11a | |
| 12.2SXD | 12.2(18)SXD7a | |
| 12.2SXE | Все версии 12.2SXE исправлены | |

| | |
|---|---|
| 12.2SXF | Все версии 12.2SXF исправлены |
| 12.2SY | Уязвима, необходима миграция на 12.2(17d)SXB11a или выше |
| 12.2SZ | Уязвима, необходима миграция на 12.2(25)S или выше |
| 12.2T | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2TPC | Уязвима, обратитесь в TAC |
| 12.2XA | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XB | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XC | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2XD | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XE | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XF | Уязвима, необходима миграция на 12.3(9a)BC или выше |
| 12.2XG | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XH | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XI | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XJ | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XK | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XL | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XM | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XN | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XQ | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XR | Уязвима, необходима миграция на 12.3(8) или выше |

| | |
|---|---|
| 12.2XS | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XT | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XU | Уязвима, необходима миграция на 12.3(12) или выше |
| 12.2XV | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2XW | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YA | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YB | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YC | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YD | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2YE | Уязвима, необходима миграция на 12.2(25)S или выше |
| 12.2YF | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YG | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YH | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YJ | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YK | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2YL | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2YM | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2YN | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2YO | Not vulnerable |
| 12.2YP | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YQ | Уязвима, необходима миграция на 12.3(4)T13 или выше |

| | |
|---|---|
| 12.2YR | Уязвима, необходима миграция на 12.3(4)T13 или выше |
| 12.2YS | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2YT | Уязвима, необходима миграция на 12.3(8) или выше |
| 12.2YU | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2YV | Уязвима, необходима миграция на 12.3(4)T13 или выше |
| 12.2YW | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2YX | Уязвима, необходима миграция на 12.3(14)T или выше |
| 12.2YY | Уязвима, необходима миграция на 12.3(4)T13 или выше |
| 12.2YZ | Уязвима, необходима миграция на 12.2(25)S или выше |
| 12.2ZA | Уязвима, необходима миграция на 12.2(17d)SXBa или выше |
| 12.2ZB | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2ZC | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2ZD | Уязвима, обратитесь в TAC |
| 12.2ZE | Уязвима, необходима миграция на 12.3(8) or laer |
| 12.2ZF | Уязвима, необходима миграция на 12.3(4)T13 или выше |
| 12.2ZG | Vulnerable; for SOHO9x, migrate to 12.3(8)YG2 или выше. Для c83x, необходима миграция на 12.3(2)XA3 или выше |
| 12.2ZH | Уязвима, обратитесь в TAC |
| 12.2ZJ | Уязвима, необходима миграция на 12.3(8)T или выше |
| 12.2ZL | Уязвима, обратитесь в TAC |
| 12.2ZN | Уязвима, необходима миграция на 12.3(4)T13 или выше |

| | | |
|---|---|---|
| 12.2ZP | Уязвима, необходима миграция на 12.3(8)XY или выше | |
| **Уязвимые версии на базе 12.3** | **Повторная сборка** | **Обслуживание** |
| 12.3 | | 12.3(8) |
| 12.3B | Уязвима, необходима миграция на 12.3(8)T7 или выше | |
| 12.3BC | | 12.3(9a)BC |
| 12.3BW | Уязвима, необходима миграция на 12.3(8)T или выше | |
| 12.3JA | | 12.3(8)JA |
| 12.3JEA | Все версии 12.3JEA исправлены | |
| 12.3JEB | Все версии 12.3JEA исправлены | |
| 12.3JK | 12.3(2)JK2 | 12.3(8)JK |
| 12.3JX | 12.3(7)JX6 | 12.3(11)JX |
| 12.3T | 12.3(4)T13 | 12.3(8)T |
| | Поддержка платформ ограниченна: обратитесь в TAC | |
| | Необходима миграция на 12.4(1) или выше | |
| 12.3TPC | 12.3(4)TPC11b | |
| 12.3XA | 12.3(2)XA6 | |
| 12.3XB | Уязвима, необходима миграция на 12.3(8)T или выше | |
| 12.3XC | Уязвима, обратитесь в TAC | |
| 12.3XD | Уязвима, необходима миграция на 12.3(8)T7 или выше | |
| 12.3XE | Уязвима, обратитесь в TAC | |

| | | |
|---|---|---|
| 12.3XF | Уязвима, необходима миграция на 12.3(11)T или выше | |
| 12.3XG | Уязвима, обратитесь в TAC | |
| 12.3XH | Уязвима, необходима миграция на 12.3(11)T или выше | |
| 12.3XI | 12.3(7)XI8 | |
| 12.3XJ | Уязвима, необходима миграция на 12.3(8)XW или выше | |
| 12.3XK | Уязвима, необходима миграция на 12.3(14)T или выше | |
| 12.3XQ | Уязвима, необходима миграция на 12.4(1) или выше | |
| 12.3XR | Все версии 12.3XR исправлены | |
| 12.3XS | Все версии 12.3XS исправлены | |
| 12.3XU | Все версии 12.3XU исправлены | |
| 12.3XW | Все версии 12.3XW исправлены | |
| 12.3XX | Все версии 12.3XX исправлены | |
| 12.3XY | Все версии 12.3XR исправлены | |
| 12.3YA | Все версии 12.3YA исправлены | |
| 12.3YD | Все версии 12.3YD исправлены | |
| 12.3YF | Все версии 12.3YF исправлены | |
| 12.3YG | Все версии 12.3YG исправлены | |
| 12.3YH | Все версии 12.3YH исправлены | |
| 12.3YI | Все версии 12.3YI исправлены | |
| 12.3YJ | Все версии 12.3YJ исправлены | |
| 12.3YK | Все версии 12.3YK исправлены | |

| | | |
|---|---|---|
| 12.3YM | Все версии 12.3YM исправлены | |
| 12.3YQ | Все версии 12.3YQ исправлены | |
| 12.3YS | Все версии 12.3YS исправлены | |
| 12.3YT | Все версии 12.3YT исправлены | |
| 12.3YU | Все версии 12.3YU исправлены | |
| 12.3YX | Все версии 12.3YX исправлены | |
| 12.3YZ | Все версии 12.3YZ исправлены | |
| **Узявимые версии на базе 12.4** | **Повторная сборка** | **Обслуживание** |
| Все версии 12.4 исправлены | | |

| **Версия Cisco IOS XR** | **SMU ID** | **Установочные пакеты** |
|---|---|---|
| 3.2.2 для CRS-1 | AA01482 | hfr-base-3.2.2.CSCeh52410.pie |
| 3.2.3 для CRS-1 | AA01483 | hfr-base-3.2.3.CSCeh52410.pie |
| 3.2.4 для CRS-1 | AA01484 | hfr-base-3.2.4.CSCeh52410.pie |
| 3.2.6 для CRS-1 | AA01727 | hfr-base-3.2.6.CSCeh52410.pie |
| 3.3.x для CRS-1 и XR12000 | Исправлена | |
| 3.4.x для CRS-1 и XR12000 | Исправлена | |

Установочные пакеты IOS XR (PIE) можно загрузить по адресу http://www.cisco.com/cgi-bin/tablebuild.pl/iosxr-smu?sort=release (только для зарегистрированных заказчиков) . Инструкции по установке можно найти в сопроводительных TXT-файлах.

## Временные решения

Дополнительные варианты уменьшения воздействия проблемы, которые можно использовать на устройствах Cisco в сети, доступны в сопроводительном документе Cisco Applied Intelligence для этой рекомендации. Адрес:

http://www.cisco.com/warp/public/707/cisco-air-20070124-crafted-ip-option.shtml

### Избирательное отбрасывание параметров IP

Функция избирательного отбрасывания параметров IP позволяет маршрутизаторам Cisco снизить воздействие параметров IP, отбрасывая пакеты, которые их содержат, или не обрабатывая (игнорируя) эти параметры в пакете.

Наиболее эффективным временным решением будет использование параметра "drop" следующей глобальной команды конфигурации. **ip options drop**. Эта команда позволяет отбрасывать все IP-пакеты, которые содержат параметры IP и адресованы маршрутизатору или являются транзитными, до того, как они будут обработаны. Это позволяет предотвратить использование уязвимости как локально, так и на узлах более низкого уровня.

Избирательное отбрасывание параметров IP доступно в ПО Cisco IOS, начиная с версий 12.0(23)S для 12000, 12.0(32)S для 10720 и 12.3(4)T, 12.2(25)S и 12.2(27)SBC для других платформ.

Обратите внимание, что использование этой команды приведет к отбрасыванию разрешенных IP-пакетов. В числе протоколов, которые могут пострадать это этого RSVP (используется Microsoft NetMeeting), MPLS TE, MPLS OAM, DVMRP, IGMPv3, IGMPv2 и разрешенный протокол PGM.

**Примечание:** Параметр **ignore** глобальной команды **ip options ignore**, который доступен только для маршрутизатора Cisco 12000, 12.0(23)S, НЕ является временным решением для данной проблемы.

Дополнительные сведения об избирательном отбрасывании параметров IP доступны по адресу http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00801d4a94.html.

### Транзитные списки контроля доступа (ACL)

Настройте список ACL на блокировку трафика следующих типов:

- Эхо-запрос (Ping) ICMP тип 8
- Временная метка ICMP тип 13
- Информационный запрос ICMP тип 15
- Запрос маски адреса ICMP тип 17
- Протокол IP PIM 103
- Протокол IP PGM IP 113
- TCP-порт 465 протокола URD (URL Rendezvous Directory)

Протокол ICMP входит в семейство протоколов TCP/IP и используется для сообщения о неисправных состояниях и предоставления диагностических данных. Фильтрация сообщений ICMP может повлиять на отчеты о неисправных состояниях и диагностические отчеты, в том числе на команды команды "ping" и "traceroot" ОС Windows, которые используют эхо-запросы ICMP.

Если устройство настроено на обработку PIM, PGM или URD, блокирование этих пакетов нарушит разрешенную работу данных протоколов.

Поскольку IP-адрес источника этих пакетов можно легко подделать, трафик, подверженный влиянию проблемы, необходимо блокировать на всех IPv4-интерфейсах устройства.

Список ACL ниже специально разработан для блокировки трафика атак. Его необходимо применить на всех IPv4-интерфейсах устройства, добавив фильтры, настроенные для конкретной топологии:

```
access-list 150 deny   icmp any any echo
access-list 150 deny   icmp any any information-request
access-list 150 deny   icmp any any timestamp-request
access-list 150 deny   icmp any any mask-request
access-list 150 deny   tcp any any eq 465
```

```
access-list 150 deny   103 any any
access-list 150 deny   113 any any
access-list 150 permit ip any any

interface serial 2/0
ip access-group 150 in
```

Эти инструкции ACL следует развертывать на периферии сети в рамках транзитного списка доступа, который защищает маршрутизатор, на котором настроен список ACL, а также на всех устройствах за ним. Дополнительные сведения о транзитных списках ACL можно найти в публикации "Транзитные списки контроля доступа: фильтрация на периферии", которая доступна по адресу http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml.

Следующий список ACL для Cisco IOS XR специально разработан для блокировки трафика атак. Его необходимо применить на всех IPv4-интерфейсах устройства, добавив фильтры, настроенные для конкретной топологии:

```
ipv4 access-list ios-xr-transit-acl
10 deny   icmp any any echo
20 deny   icmp any any information-request
30 deny   icmp any any timestamp-request
40 deny   icmp any any mask-request
50 deny   tcp any any eq 465
60 deny   103 any any
70 deny   113 any any
80 permit ip any any

interface POS 0/2/0/
 ipv4 access-group ios-xr-transit-acl ingress
```

Сведения о настройке списков доступа в ОС Cisco IOS XR доступны по адресу http://www.cisco.com/en/US/products/ps5763/products_command_reference_chapter09186a00803e01ae.html.

## Инфраструктурные списки ACL

Несмотря на то, что заблокировать трафик, проходящий через сеть, довольно сложно, существует возможность определить трафик, который ни при каких обстоятельствах не должен отправляться устройствам инфраструктуры, и заблокировать его на границах сети. Инфраструктурные списки ACL считаются лучшим методом обеспечения безопасности сети и должны рассматриваться как долгосрочное дополнение к системе безопасности, а также в качестве средства устранения рассматриваемой уязвимости. Пример ACL, приведенный ниже, следует использовать как часть инфраструктурного списка доступа, который будет защищать устройства с IP-адресами из диапазона IP-адресов инфраструктуры.

### Cisco IOS

```
access-list 150 deny   icmp any INFRASTRUCTURE_ADDRESSES echo
access-list 150 deny   icmp any INFRASTRUCTURE_ADDRESSES information-request
access-list 150 deny   icmp any INFRASTRUCTURE_ADDRESSES timestamp-request
access-list 150 deny   icmp any INFRASTRUCTURE_ADDRESSES mask-request
access-list 150 deny   tcp any INFRASTRUCTURE_ADDRESSES  eq 465
access-list 150 deny   103 any INFRASTRUCTURE_ADDRESSES
access-list 150 deny   113 any INFRASTRUCTURE_ADDRESSES
access-list 150 permit ip any any

interface serial 2/0
ip access-group 150 in
```

### Cisco IOS XR

```
ipv4 access-list ios-xr-infrastructure-acl
10 deny   icmp any INFRASTRUCTURE_ADDRESSES  echo
20 deny   icmp any INFRASTRUCTURE_ADDRESSES  information-request
30 deny   icmp any INFRASTRUCTURE_ADDRESSES  timestamp-request
40 deny   icmp any INFRASTRUCTURE_ADDRESSES  mask-request
50 deny   tcp any INFRASTRUCTURE_ADDRESSES  eq 465
```

```
60 deny   103 any INFRASTRUCTURE_ADDRESSES
70 deny   113 any INFRASTRUCTURE_ADDRESSES
80 permit ip any any

interface POS 0/2/0/2
 ipv4 access-group ios-xr-infrastructure-acl ingress
```

Статья под названием "Защита ядра: Списки контроля доступа для защиты инфраструктуры" содержит указания и рекомендуемые методики развертывания списков доступа. Статья доступна по адресу http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml.

Сведения о настройке списков доступа в ОС Cisco IOS XR доступны по адресу http://www.cisco.com/en/US/products/ps5763/products_command_reference_chapter09186a00803e01ae.html.

### Списки ACL на получение

В распределенных платформах, начиная с версий ПО Cisco IOS 12.0(21)S2 для 12000 (GSR), 12.0(24)S для 7500 и 12.0(31)S, для 10720 можно использовать списки ACL на получение. Списки ACL на получение защищают устройство от вредоносного трафика до того, как он может оказать влияние на процессор маршрутизации. Список ACL на получение разработан для защиты только устройства, на котором он задан. На модели 12000 транзитный трафик никогда не затрагивается списком ACL на получение. Поэтому IP-адрес назначения "any" используемый в примерах ACL ниже, относится к собственным физическим или виртуальным IP-адресам маршрутизатора. На моделях 7500 и 10720, транзитный трафик с параметрами IP будет принят или отклонен в соответствии с настройками списка ACL на получение. Списки ACL на получение считаются лучшим методом обеспечения безопасности сети и должны рассматриваться как долгосрочное дополнение к системе безопасности, а также в качестве средства устранения рассматриваемой уязвимости.

Статья под названием "GSR: списки ACL на получение" поможет идентифицировать и разрешить легальный трафик и отклонить весь нежелательный трафик. Статья доступна по адресу http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml

Список ACL на получение, представленный ниже, разработан специально для блокировки трафика атаки:

```
access-list 101 deny   icmp any any echo
access-list 101 deny   icmp any any information-request
access-list 101 deny   icmp any any timestamp-request
access-list 101 deny   icmp any any mask-request
access-list 101 deny   tcp any any eq 465
access-list 101 deny   103 any any
access-list 101 deny   113 any any
access-list 101 permit ip any any
!
ip receive access-list 101
```

### Политики плоскости управления

Для снижения воздействия уязвимости можно использовать функцию политик плоскости управления (CoPP). В примере ниже все пакеты, которые могут использовать уязвимость, отклоняются, в то время как весь остальной IP-трафик принимается. Из-за способа обработки пакетов с параметрами IP, функция CoPP применяется к пакетам, адресованным самому маршрутизатору, и транзитным пакетам, которые проходят через маршрутизатор на пути к IP-адресу назначения. Это относится ко всем платформам, кроме 12000, в которой будут отбрасываться только пакеты атаки, адресованные самому маршрутизатору.

```
access-list 100 permit icmp any any echo
access-list 100 permit icmp any any information-request
access-list 100 permit icmp any any timestamp-request
access-list 100 permit icmp any any mask-request
access-list 100 permit tcp any any eq 465
access-list 100 permit 103 any any
access-list 100 permit 113 any any
access-list 100 deny   ip any any
!
class-map match-all drop-options-class
match access-group 100
```

```
!
!
policy-map drop-options-policy
class drop-options-class
  drop
!
control-plane
service-policy input drop-options-policy
```

Обратите внимание, что в последовательностях версий Cisco IOS 12.0S, 12.2S и 12.2SX, синтаксис карты политик будет другим:

```
policy-map drop-options-policy
class drop-options-class
police 32000 1500 1500 conform-action drop exceed-action drop
```

Из-за способа обработки пакетов с параметрами IP, функция CoPP применяется к пакетам, адресованным самому маршрутизатору, и транзитным пакетам, которые проходят через маршрутизатор на пути к IP-адресу назначения. В примере ниже отклоняются только пакеты с параметрами IP, которые могут использовать уязвимость и адресуются самому маршрутизатору или являются транзитными. Весь остальной IP-трафик разрешается.

```
ip access-list extended drop-affected-options
permit icmp any any echo option any-options
permit icmp any any information-request option any-options
permit icmp any any timestamp-request option any-options
permit icmp any any mask-request option any-options
permit pim any any option any-options
permit 113 any any option any-options
permit tcp any any eq 465 option any-options
deny ip any any
!
class-map match-all drop-options-class
match access-group name drop-affected-options
!
!
policy-map drop-opt-policy
class drop-options-class
 drop
!
control-plane
service-policy input drop-opt-policy
```

Обратите внимание, что в последовательности версий Cisco IOS 12.2S синтаксис карты политик будет другим:

```
policy-map drop-opt-policy
class drop-options-class
 police 32000 1500 1500 conform-action drop exceed-action drop
```

Функция CoPP доступна в последовательностях версий Cisco IOS 12.0S, 12.2SX, 12.2S, 12.3T, 12.4 и 12.4T.

Для поддержки фильтрации параметров IP в списках ACL необходимы именованные списки ACL. Фильтрация параметров IP в списках ACL не поддерживается в версиях 12.0S и 12.2SX.

Обратите внимание, что пакеты PGM, как правило, используют параметр "Router Alert" и отбрасывание пакетов PGM с параметрами IP повлияет и на разрешенные пакеты PGM.

В примерах CoPP выше записям ACL, которые соответствуют пакетам, использующим уязвимость, назначается действие "permit". В результате эти пакеты отклоняются функцией "drop" карты политик. Пакеты, которым назначено действие "deny", не затрагиваются функцией "drop" карты политик.

См. дополнительные сведения о конфигурации и использовании CoPP по адресам

http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml и
http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a008052446b.html.

См. дополнительные сведения о фильтрации параметров IP с помощью списков доступа по адресу
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d4a7d.html.

## Получение исправленного программного обеспечения

Cisco предоставит пострадавшим заказчикам бесплатное программное обеспечение для устранения этой уязвимости. Эта рекомендация будет обновляться по мере выхода новых исправленных версий. Перед развертыванием программного обеспечения заказчикам следует проконсультироваться у своего поставщика услуг по техническому обслуживанию или проверить данные о совместимости набора функций и известных проблемах своей среды.

Заказчики могут выполнять установку и получать поддержку только тех наборов функций, которые они приобрели. Устанавливая, загружая, получая доступ или используя эти обновления ПО любым другим способом заказчик принимает условия лицензии на ПО Cisco, доступные по адресу http://www.cisco.com/public/sw-license-agreement.html, если иное не указано на странице загрузки Cisco.com по адресу http://www.cisco.com/public/sw-center/sw-usingswc.shtml.

Для получения обновлений ПО не следует обращаться по адресам "psirt@cisco.com" и "security-alert@cisco.com".

## Заказчики с договорами на обслуживание

Заказчики с договорами на обслуживание получают обновленное ПО через обычные каналы распространения обновлений. Для большинства заказчиков это означает, что обновления можно получить в разделе Software Center глобального веб-узла Cisco по адресу http://www.cisco.com.

## Заказчики, работающие со сторонними организациями по поддержке

Заказчики с продуктами Cisco, которые поставлены и обслуживаются в соответствии с прежним или текущим соглашением со сторонними организациями, например партнерами Cisco, авторизованными торговыми посредниками или поставщиками услуг, должны обратиться в организацию по поддержке за инструкциями и помощью в выборе наилучшего плана действий в связи с этой рекомендацией.

Эффективность того или иного временного решения проблемы или исправления зависит от условий конкретной среды заказчика, таких как сочетание продуктов, топология сети, поведение трафика и задачи организации. Поскольку проблема затрагивает обширный набор продуктов и версий, заказчикам следует проконсультироваться с поставщиком услуг или организацией по поддержке, чтобы убедиться, что выбранное временное решение или исправление является наилучшим для использования в намеченной сети, перед их развертыванием.

## Заказчики без договоров на обслуживание

Заказчики, которые приобрели продукты у Cisco, но не имею договора на обслуживания, а также заказчики, которые приобрели продукты у сторонних компаний, но не смогли получить обновления у продавца должны обратиться в центр технической поддержки (TAC). Контактные сведения TAC:

- +1 800 553 2447 (звонки из Северной Америки бесплатны)
- +1 408 526 7209 (звонки из любой точки земного шара бесплатны)
- Электронная почта: tac@cisco.com

Подготовьте серийный номер продукта и предоставьте URL-адрес этого уведомления в качестве доказательства вашего права на бесплатное обновление. Бесплатные обновления для заказчиков без договора на обслуживание необходимо получать через TAC.

См. дополнительные сведения о TAC, в том числе специальные локализованные номера телефона, инструкции и адреса электронной почты для различных языков по адресу http://www.cisco.com/web/RU/support/content/tsd_cisco_worldwide_contacts.html.

## Использование уязвимости и публичные сообщения

Службе Cisco PSIRT неизвестно о публичных сообщениях о злонамеренном использовании уязвимости, описанной в этой рекомендации. Эта уязвимость была обнаружена во время внутреннего тестирования.

## Состояние уведомления: ОКОНЧАТЕЛЬНО

НАСТОЯЩИЙ ДОКУМЕНТ ПРЕДСТАВЛЕН "КАК ЕСТЬ" И НЕ ПОДРАЗУМЕВАЕТ НИКАКИХ ГАРАНТИЙ, В ТОМ ЧИСЛЕ ГАРАНТИЙ ТОВАРОПРИГОДНОСТИ ИЛИ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ. ВЫ ПРИНИМАЕТЕ НА СЕБЯ ВСЕ РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ НАСТОЯЩЕГО ДОКУМЕНТА ИЛИ МАТЕРИАЛОВ, НА КОТОРЫЕ ЗДЕСЬ ПРИВОДЯТСЯ ССЫЛКИ. CISCO ОСТАВЛЯЕТ ЗА СОБОЙ ПРАВО ВНОСИТЬ ИЗМЕНЕНИЯ ИЛИ ОБНОВЛЯТЬ НАСТОЯЩИЙ ДОКУМЕНТ В ЛЮБОЕ ВРЕМЯ.

Отдельная копия или парафраз текста этого документа, в которых пропущены URL-адреса распространения в разделе ниже, являются неуправляемой копией. В ней может отсутствовать важная информация. Кроме того, такая копия может содержать фактические ошибки.

## Распространение

Эта рекомендация опубликована на глобальном веб-узле Cisco по адресу:

http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

В дополнение к публикации на глобальном веб-узле, этот текст подписан PGP-ключом Cisco PSIRT и распространен среди следующих получателей новостей по электронной почте и через Usenet.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Будущие обновления, если таковые появятся, будут опубликованы на глобальном веб-узле Cisco, но могут быть не объявлены участникам списков рассылки и новостных групп. Пользователям, которых беспокоит эта проблема, рекомендуется проверять наличие обновлений по указанному URL-адресу.

## История редакций

| | | |
|---|---|---|
| Редакция 1.3 | 2 февраля 2007 г. | Обновлены записи версий 12.0W и 12.1EO в таблице версий и исправлений программного обеспечения. |
| Редакция 1.2 | 27 января 2007 г. | Обновлена таблица ПО Cisco IOS. |
| Редакция 1.1 | 25 января 2007 г. | В разделе "Версии и исправления программного обеспечения" добавлены сведения об установочных пакетах (PIE) в таблицу Cisco версий IOS XR. |
| Редакция | 24 января | |

| | | |
|---|---|---|
| 1.0 | 2007 г. | Начальный общедоступный выпуск документа. |

## Процедуры безопасности Cisco

Полные сведения о процедуре создания отчетов об уязвимостях продуктов Cisco, помощи в разрешении инцидентов, связанных с безопасностью и регистрации для получения информации Cisco, связанной с безопасностью, можно найти на глобальном веб-узле Cisco по адресу http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. Кроме того, на этой странице доступны инструкции по получению уведомлений о безопасности Cisco. Все рекомендации Cisco по вопросам безопасности доступны по адресу http://www.cisco.com/go/psirt.



Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/97439/cisco-sa-20070124-crafted-ip-option.shtml