Содержание

Введение

Существует возможная атака типа отказ в обслуживании в интернет-провайдерах, которая предназначается для сетевых устройств.

- **Атака диагностического порта Протокола UDP:** отправитель передает громкость запросов о диагностическом обслуживании UDP на маршрутизаторе. Это заставляет все ресурсы ЦПУ быть использованными для обрабатывания фальшивых запросов.

Этот документ описывает, как потенциальная атака диагностического порта UDP происходит и предлагает, чтобы методы использовали с программным обеспечением Cisco IOS, для защиты от него.

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. Некоторые команды, упомянутые в этом документе, являются только доступным началом в Cisco IOS Software Release 10.2 (9), 10.3 (7), и 11.0 (2), и все последующие релизы. Эти команды являются по умолчанию в программном обеспечении Cisco IOS версии 12.0 и позже.

Условные обозначения

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

Описание проблемы

Атака на диагностический порт протокола UDP

По умолчанию маршрутизатор Cisco имеет серию портов диагностики, включенных для определенного UDP и сервисов TCP. Эти сервисы включают эхо, chargen и сброс. Когда хост подключает к этим портам, малая величина возможностей ЦПУ использована для обрабатывания этих запросов.

Если одиночное устройство нападения передает большое заграждение запросов с другим, случайным, IP-адресами ложного источника, возможно, что маршрутизатор Cisco становится разбитым и замедляется или отказывает.

: (%SYS-3 NOPROC) CPU. **Процесс exec command show** показывает много процессов с тем же названием, таких как "Эхо UDP".

Защитите от атак непосредственно к сетевым устройствам

Отключите порты диагностики UDP

Любое сетевое устройство, которое имеет UDP и диагностическое обслуживание TCP, должно быть защищено межсетевым экраном или отключать сервисы. Для маршрутизатора Cisco это можно выполнить с помощью команд глобальной конфигурации.

```
no service udp-small-serversno service tcp-small-servers
```

См. Приложение для дополнительных сведений об этих командах. Команды доступны в Cisco IOS Software Releases 10.2(9), 10.3(7), и 11.0(2) и выше. Эти команды являются по умолчанию в программном обеспечении Cisco IOS версии 12.0 и позже.

Предотвратите сеть от невольного хостинга атаки

Поскольку первичным механизмом DoS-атак (отказа в обслуживании) является генерация трафика с разных IP-адресов, компания Cisco рекомендует фильтрацию трафика, передающегося в Интернет. Основной принцип — отбрасывать пакеты с недопустимыми исходными IP-адресами, по мере того как они поступают в Интернет. Это не предотвращает атаку отказ в обслуживании в вашей сети. Однако это помогает подвергшимся нападению сторонам исключать собственное расположение как источник атакующего. Кроме того, это обеспечивает защиту сети от атак подобного класса.

Предотвратите передачу недопустимых IP - адресов

С помощью фильтрации пакетов на маршрутизаторах, которые соединяют вашу сеть с Интернетом, вы можете разрешить выход в интернет только пакетам с допустимыми IP-адресами отправителей.

Например, если ваша сеть состоит из, сеют 172.16.0.0, и ваши подключения

маршрутизатора к вашему интернет-провайдеру с помощью интерфейса FDDI0/1, можно применить список доступа как это:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 anyaccess-list 111 deny ip any any log
[1]interface Fddi 0/1ip access-group 111 out
```

[1]последняя линия списка доступа определяет, существует ли какой-либо трафик с недопустимым адресом источника, который вводит Интернет. Это помогает определять местоположение источника возможных атак.

Предотвратите прием недопустимых IP - адресов

Для ISP, обслуживающих конечные сети, Cisco настоятельно рекомендует подтверждение входящих пакетов от клиентов. Это можно выполнить, используя фильтры входящих пакетов на своих граничных маршрутизаторах.

Например, если вашим клиентам подключили эти номера сетей с вашим маршрутизатором через интерфейс FDDI под названием "FDDI 1/0", можно создать этот список доступа.

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0access-list 111 permit ip
192.168.0.0 0.0.15.255 anyaccess-list 111 permit ip 172.18.0.0 0.0.255.255 anyaccess-list 111
deny ip any any loginterface Fddi 1/0ip access-group 111 in
```

Примечание: Последняя линия списка доступа определяет, существует ли какой-либо трафик с недопустимым адресом источника, который вводит Интернет. Это помогает определять местоположение источника возможной атаки.

Приложение: Описание маленьких серверов

Маленькие серверы являются серверами (демоны, в термине Unix), которые работают в маршрутизаторе, которые полезны для диагностики. Однако они существуют по умолчанию.

Ниже представлены команды для малых серверов TCP и UDP:

- **service tcp-small-servers**
- **service udp-small-servers**

Если вы не хотите, чтобы ваш маршрутизатор предоставил какие-либо службы без поддержки маршрутизации, выключите их (использование **никакой** формы предыдущих команд).

Маленькие серверы TCP:

- **Эхо**? Реагирует на то, что вы вводите. **Для просмотра наберите команду telnet x.x.x.x echo.**
- **Chargen**? Создает поток данных в формате ASCII. Введите **chargen команды telnet x. x . x . x** для наблюдения.
- **Сброс**? Отбрасывает все введенные данные. **Введите команду telnet x.x.x.x discard, чтобы увидеть это.**
- **Дневное время**? Возвращает системную дату и время, если корректный. Если вы выполняете NTP или установили дату и времю вручную от уровня exec, это корректно. **Введите команду telnet x.x.x.x daytime для отображения.**

Малые серверы UDP:

- **Эхо**? Повторяет информационное наполнение дейтаграммы, которую вы передаете.
- **Сброс**? Тихо передает дейтаграмму, которую вы передаете.
- **Chargen**? Сбрасывает отправленную датаграмму и отвечает 72-символьной строкой символов ASCII, заканчивающейся специальными символами CR+LF.

Примечание: Почти все серверы доступа корпоративной сети под управлением Unix поддерживают маленькие серверы, ранее перечисленные. Маршрутизатор также предлагает сервис Finger и сервис протокола BOOTP асинхронной линии. Они могут быть независимо выключены с **finger no service** команд global конфигурации и **no ip bootp server**, соответственно.

Дополнительные сведения

- ПО Cisco IOS)
- Техническая поддержка - Cisco Systems