УДК 004.738.5

# ОТКАЗ В ОБСЛУЖИВАНИИ ЧЕРЕЗ IPV6

Стасивский Л.С.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, stasivskyj@gmail.com

**В данной работе рассмотрена атака типа “отказ в обслуживании” через протокол IPv6 и приведен способ защиты от нее.**

***Ключевые слова – файрвол; RA-флудер.***

Протокол IPv4 в настоящее время столкнулся с рядом проблем, таких как проблема масштабируемости сети, неприспособленность протокола к передаче мультисервисной информации с поддержкой различных классов обслуживания, включая обеспечение информационной безопасности. Указанные проблемы обусловили развитие классической версии протокола IPv4 в направлении разработки версии IPv6, которая у большинства современных сетевых систем по умолчанию включена.

IPv6 также несет новые возможности, но с ними и новые векторы атак, и новые уязвимости. Простейший пример: когда есть некий файрвол, который осуществляет правильную фильтрацию. Проблема в том, что фильтрация происходит только для IPv4, а в то же время IPv6 обделена таким вниманием.

И значит, злоумышленник может проводить все свои атаки, просто перейдя на IPv6-адресацию.

Несколько лет назад разработчики из разных стран начали усердно изучать IPv6 и нашли “пучок” различных ошибок. Одной из таких стала такое понятие – ICMPv6 Router Announcements flood.

Router Announcements (RA) в легальных целях используется для того, чтобы, когда к подсети подключился новый маршрутизатор, он мог бы обозначить свое появление другим хостам. Например: «я такой-то и отвечаю за такую-то подсеть». И все хосты, получив такой пакет, обновляют свои таблицы маршрутизации, добавляя новые данные. Кроме этого, RA может быть использована для некой замены DHCP. И когда в ОС установлена возможность автоматического получения IP, при получении RA ОС также будет пытаться получить IP-адрес в новой подсети.

Большинство ОС по умолчанию имеют включенный IPv6, а также поддерживают автоматическое получение настроек. Таким образом, для атаки требуется послать в подсеть много рандомных RA-пакетов, и хосты, получая их, будут обновлять таблицы маршрутизации.

Но самое опасное в том, что на обновление их уходит очень много ресурсов и в итоге ОС перестает нормально работать. К примеру, на среднестатистическом домашнем компьютере с ОС Windows которая “поедает” всю память и занимает все процессорное время. Аналогичная ситуация есть с FreeBSD, а также с сетевыми девайсами Juniper и Cisco! Причем тот же Microsoft сообщил, что они не будут исправлять эту ошибку. Вероятно, это связано с тем, что для устранения уязвимости нужно отказаться от поддержки RA или фильтровать их как-то, а тогда получается отклонение от стандартов.

Теперь практика. Существует большой набор утилит, нацеленных на IPv6, включающий в себя и RA-флудер. Таким образом, нужно всего лишь скачать программы и выполнить команду (для BackTrack):

*flood_router6 eth0*

где ethO – интерфейс, куда посылать пакеты.

Перед проведением атаки нужно защитить и себя – так как пакеты широковещательные, а потому обрабатываются всеми девайсами в сети.

Немного о защите от RA для Windows. Самое простое решение – отключить IPv6. Но можно и просто отключить поддержку RA-пакетов следующей командой:

*netsh interface ipv6 set interface "Local Area – Connection" routerdiscovery=disabled*

Стоит еще отметить и то, что из-за опасности атак стали появляться различные программы для защиты от RA flood'a. Но и для них уже придумали пути обхода – в основном за счет манипуляций фрагментацией пакетов.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Интернет статья: Win 7 DoS by RA Packets / Способ доступа: URL: http://samsclass.info/ipv6/proj/flood-router6a.htm. – Win 7 DoS by RA Packets.

2. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атаки через INTERNET. —СПб.: НПО "Мир и семья 95" Серия учебной литературы "МАГИСТР", 1997.