

Network Working Group  
Request for Comments: 5095  
Updates: 2460, 4294  
Category: Standards Track

J. Abley  
Afilias  
P. Savola  
CSC/FUNET  
G. Neville-Neil  
Neville-Neil Consulting  
December 2007

## Отказ от заголовков Routing типа 0 в IPv6 Deprecation of Type 0 Routing Headers in IPv6

### Статус документа

В этом документе приведена спецификация проекта стандартного протокола Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущий статус стандартизации протокола можно узнать из текущей версии документа Internet Official Protocol Standards (STD 1). Документ может распространяться свободно.

### Аннотация

Функциональность, обеспечиваемая в протоколе IPv6 заголовками Routing типа 0 может быть использована для «усиления» трафика через удалённые пути в целях организации DoS<sup>1</sup>-атак. Этот документ изменяет спецификацию протокола IPv6 с целью отказа от использования заголовков расширения Routing типа 0 с учётом отмеченной выше проблемы.

### Оглавление

1. Введение.....	1
2. Определения.....	2
3. Запрет RH0.....	2
4. Операции.....	2
4.1. Фильтрация на входе.....	2
4.2. Политика межсетевого экранирования.....	2
5. Вопросы безопасности.....	2
6. Взаимодействие с IANA.....	2
7. Благодарности.....	2
8. Литература.....	2
8.1. Нормативные документы.....	2
8.2. Дополнительная литература.....	2

## 1. Введение

В [RFC2460] определён заголовок расширения IPv6 Routing, идентифицируемый значением 43 в поле Next Header заголовка, непосредственно предшествующего данному заголовку. Для заголовка Routing был определён также субтип Type 0. Заголовки Routing этого типа в данном документе обозначаются RH0.

Один заголовок RH0 может включать множество адресов промежуточных узлов без запрета многократного включения адреса в один заголовок RH0. Это позволяет создавать такие пакеты, которые будут многократно осциллировать между двумя хостами или маршрутизаторами, обрабатываемыми RH0. В результате атакующий может создать поток пакетов, который будет «усиливаться» в пути, что можно использовать для создания перегрузки на произвольном удалённом пути и, следовательно, организации DoS-атак. В работе [CanSecWest07] было продемонстрировано 88-кратное усиление потока с использованием описанного метода.

Такая атака представляется серьёзной, поскольку она оказывает влияние на весь путь между вовлечёнными в атаку узлами, а не только на эти узлы или их локальные сети. Аналогичная функциональность обеспечивается опцией source route протокола IPv4, но возможности злоупотребления RH0 существенно выше, поскольку этот заголовок позволяет задать большее число промежуточных узлов в каждом пакете.

Важность этой угрозы представляется достаточно серьёзной, чтобы полностью отказаться от использования RH0. Побочным эффектом отказа от этого заголовка является исключение продуктивного использования RH0, однако эту проблему можно будет решить в будущих спецификациях заголовка Routing.

Потенциальные проблемы, связанные с RH0 были обнаружены в 2001 году [Security]. В 2002 году было предложено ограничить обработку заголовков Routing на хостах [Hosts]. Эти предложения привели к изменению спецификации Mobile IPv6 с использованием заголовков Routing типа 2 взамен RH0 [RFC3775]. Vishwas Manral идентифицировал различные риски, связанные с RH0 в 2006 году. Эти риски включают атаки с усилением; некоторые уязвимости описаны (наряду с другими проблемами) позднее в документе [RFC4942].

Обзор влияния RH0 на операционную безопасность представили Philippe Biondi и Arnaud Ebalard на конференции CanSecWest в Ванкувере в 2007 году [CanSecWest07]. Это выступление привело к широкому распространению информации о рисках, связанных с RH0.

Этот документ служит обновлением для [RFC2460] и [RFC4294].

<sup>1</sup>Denial-of-service - атака, нацеленная на отказ служб.

## 2. Определения

RH0 в этом документе обозначает заголовок расширения IPv6 типа 43 (Routing Header), вариант 0 (Type 0 Routing Header), определённого в [RFC2460].

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с [RFC2119].

## 3. Запрет RH0

Узлу IPv6, получающему пакет со своим адресом в поле получателя и заголовком RH0, **недопустимо** выполнять алгоритм, приведённый в конце параграфа 4.4 документа [RFC2460] для RH0. Вместо этого такие пакеты **должны** обрабатываться в соответствии с описанием параграфа 4.4 работы [RFC2460] для дейтаграмм с неизвестным значением Routing Type, а именно:

если Segments Left = 0, узел должен игнорировать заголовок Routing и перейти к обработке следующего заголовка в пакете, тип которого указан полем Next Header в заголовке Routing;

если значение поля Segments Left отлично от нуля, узел должен отбросить пакет и передать сообщение ICMP Parameter Problem с кодом 0 (указывает на нераспознанное значение Routing Type) по адресу Source Address.

От реализаций IPv6 больше не требуется обязательная реализация RH0.

## 4. Операции

### 4.1. Фильтрация на входе

Предполагается, что пройдёт некоторое время, пока все узлы IPv6 будут обновлены с прекращением поддержки RH0. Некоторые из описанных в [CanSecWest07] злоупотреблений RH0 могут быть ослаблены за счёт фильтрации на входе, как рекомендовано в [RFC2827] и [RFC3704].

В политике безопасности сайта, направленной на защиту от атак с использованием RH0, **следует** включить входную фильтрацию на границе сайта.

### 4.2. Политика межсетевого экранирования

Блокирование всех пакетов IPv6 с заголовками Routing (вместо блокирования типа 0 и разрешения остальных типов) окажет очень серьёзное влияние на будущее развитие IPv6. Если даже малая часть межсетевых экранов будет по умолчанию блокировать другие типы заголовков Routing, это лишит возможности расширения заголовков IPv6 Routing на практике. Например, Mobile IPv6 [RFC3775] базируется на использовании заголовков Routing типа 2 и широкомасштабное блокирование заголовков Routing без учёта их типа не позволит развернуть Mobile IPv6.

В политике межсетевого экранирования, предназначенной для защиты от пакетов с RH0, **недопустимо** просто отфильтровывать весь трафик с заголовками Routing; должна обеспечиваться возможность запрета пересылки трафика с заголовками типа 0 без блокирования заголовков Routing других типов. В дополнение к этому принятая по умолчанию конфигурация **должна** разрешать пересылку трафика, использующего заголовки Routing отличных от 0 типов.

## 5. Вопросы безопасности

Целью этого документа является отказ от использования в IPv6 функции, которая может оказывать нежелательное влияние на безопасность. Конкретные примеры уязвимостей, которые возникают при использовании RH0, можно найти в работе [CanSecWest07]. В частности, предоставляет механизм RH0 усиления трафика, которая может быть использована для организации DoS-атак. Описание этой функциональности приведено в разделе 1.

## 6. Взаимодействие с IANA

Реестр IANA «Internet Protocol Version 6 (IPv6) Parameters» следует обновить для отражения отказа от использования варианта 0 для заголовков IPv6 типа 43 (Routing Header).

## 7. Благодарности

В подготовку этого документа внесли свой вклад многие члены рабочих групп IPv6 и V6OPS, включая Jari Arkko, Arnaud Ebalard, Tim Enos, Brian Haberman, Jun-ichiro Itojun Hagino, Bob Hinden, Thomas Narten, Jinmei Tatuya, David Malone, Jeroen Massar, Dave Thaler и Guillaume Valadon.

## 8. Литература

### 8.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.

[RFC4294] Loughney, J., "IPv6 Node Requirements", RFC 4294, April 2006.

### 8.2. Дополнительная литература

[CanSecWest07] Biondi, P. and A. Ebalard, "IPv6 Routing Header Security", CanSecWest Security Conference 2007, April 2007. [http://www.secdev.org/conf/IPv6\\_RH\\_security-csw07.pdf](http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf)

[Hosts] Savola, P., "Note about Routing Header Processing on IPv6 Hosts", Work in Progress, February 2002.

- [RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, [RFC 2827](#), May 2000.
- [RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, [RFC 3704](#), March 2004.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [RFC4942] Davies, E., Krishnan, S., and P. Savola, "IPv6 Transition/Co-existence Security Considerations", RFC 4942, September 2007.
- [Security] Savola, P., "Security of IPv6 Routing Header and Home Address Options", Work in Progress, March 2002.

#### Адреса авторов

##### Joe Abley

Afilias Canada Corp.  
Suite 204, 4141 Yonge Street  
Toronto, ON M2P 2A8  
Canada  
Phone: +1 416 673 4176  
EMail: [jabley@ca.afilias.info](mailto:jabley@ca.afilias.info)

##### Pekka Savola

CSC/FUNET  
Espoo,  
Finland  
EMail: [psavola@funet.fi](mailto:psavola@funet.fi)

##### George Neville-Neil

Neville-Neil Consulting  
2261 Market St. #239  
San Francisco, CA 94114  
USA  
EMail: [gnn@neville-neil.com](mailto:gnn@neville-neil.com)

#### Перевод на русский язык

Николай Малых  
[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)

#### Полное заявление авторских прав

##### Copyright (C) The IETF Trust (2007).

К этому документу применимы права, лицензии и ограничения, указанные в BCP 78, и, за исключением указанного там, авторы сохраняют свои права.

Этот документ и содержащаяся в нем информация представлены "как есть" и автор, организация, которую он/она представляет или которая выступает спонсором (если таковой имеется), Internet Society и IETF отказываются от каких-либо гарантий (явных или подразумеваемых), включая (но не ограничиваясь) любые гарантии того, что использование представленной здесь информации не будет нарушать чьих-либо прав, и любые предполагаемые гарантии коммерческого использования или применимости для тех или иных задач.

#### Интеллектуальная собственность

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах RFC можно найти в BCP 78 и BCP 79.

Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить из сетевого репозитория IETF IPR по ссылке <http://www.ietf.org/ipr>.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).