

Network Working Group
Internet-Draft
Updates: [2460](#) (if approved)
Intended status: Standards Track
Expires: November 17, 2007

J. Abley
Afilias
P. Savola
CSC/FUNET
G. Neville-Neil
Neville-Neil Consulting
May 16, 2007

Deprecation of Type 0 Routing Headers in IPv6
draft-ietf-ipv6-deprecate-rh0-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on November 17, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

The functionality provided by IPv6's Type 0 Routing Header can be exploited in order to perform remote network discovery, to bypass firewalls and to achieve packet amplification for the purposes of generating denial-of-service traffic. This document updates the IPv6 specification to deprecate the use of IPv6 Type 0 Routing Headers, in

the light of these security concerns.

This document updates [RFC 2460](#).

Table of Contents

- [1.](#) Introduction [3](#)
- [2.](#) Definitions [3](#)
- [3.](#) Deprecation of RHO [3](#)
 - [3.1.](#) Origination [3](#)
 - [3.2.](#) Processing [3](#)
- [4.](#) Operations [3](#)
 - [4.1.](#) Ingress Filtering [3](#)
 - [4.2.](#) Packet Filtering [4](#)
- [5.](#) Security Considerations [4](#)
- [6.](#) IANA Considerations [4](#)
- [7.](#) Acknowledgements [4](#)
- [8.](#) References [5](#)
 - [8.1.](#) Normative References [5](#)
 - [8.2.](#) Informative References [5](#)
- [Appendix A.](#) Change History [6](#)
- Authors' Addresses [6](#)
- Intellectual Property and Copyright Statements [7](#)

[1.](#) Introduction

[RFC2460] defines an IPv6 extension header called "Routing Header", identified by a Next Header value of 43 in the immediately preceding header. A particular Routing Header subtype denoted as "Type 0" is also defined. Type 0 Routing Headers are referred to as "RH0" in this document.

Use of RH0 has been shown to have unpleasant security implications, some of which are summarised in [Section 5](#). This document deprecates the use of RH0.

This document updates [\[RFC2460\]](#).

[2.](#) Definitions

RH0 in this document denotes the IPv6 Extension Header type 43 ("Routing Header") variant 0 ("Type 0 Routing Header"), as defined in [\[RFC2460\]](#).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#).

[3.](#) Deprecation of RH0

[3.1.](#) Origination

IPv6 nodes MUST NOT originate IPv6 packets containing RH0.

[3.2.](#) Processing

IPv6 nodes MUST NOT process RH0 in packets addressed to them. Such packets MUST be processed according to the behaviour specified in

[Section 4.4 of \[RFC2460\]](#) for a datagram which includes an unrecognised Routing Type value.

[4.](#) Operations

[4.1.](#) Ingress Filtering

It is to be expected that it will take some time before all IPv6 nodes are updated to remove support for RH0. Some of the uses of RH0 described in [\[CanSecWest07\]](#) can be mitigated using ingress filtering, as recommended in [\[RFC2827\]](#) and [\[RFC3704\]](#).

Abley, et al.

Expires November 17, 2007

[Page 3]

Internet-Draft

Deprecation of RH0

May 2007

[4.2.](#) Packet Filtering

Firewall policy intended to protect against packets containing RH0 should be constructed such that routing headers of other types (which may well have legitimate and benign applications) are handled on their own merits. For example, discarding all packets with any type of routing header simply as a reaction to the problems with RH0 is inappropriate, and may hamper future functionality designed using non-type 0 routing headers. For example, Mobile IPv6 uses the type 2 Routing Header [\[RFC3775\]](#).

Where filtering capabilities do not facilitate matching specific types of Routing Headers, filtering based on the presence of any Routing Headers on IPv6 routers, regardless of type, is strongly discouraged.

[5.](#) Security Considerations

The purpose of this document is to deprecate a feature of IPv6 which has been shown to have serious security implications.

Specific examples of vulnerabilities which are facilitated by the availability of RH0 can be found in [\[CanSecWest07\]](#).

[6.](#) IANA Considerations

The IANA registry "Internet Protocol Version 6 (IPv6) Parameters"

should be updated to reflect that variant 0 of IPv6 header-type 43 ("Routing Header") is deprecated.

7. Acknowledgements

Potential problems with Routing Headers were identified in 2001 [[I-D.savola-ipv6-rh-ha-security](#)]. In 2002 a proposal was made to restrict Routing Header processing in hosts [[I-D.savola-ipv6-rh-hosts](#)]. These efforts did not gain sufficient momentum to change the IPv6 specification, but resulted in the modification of the Mobile IPv6 specification to use the type 2 Routing Header instead of RH0 [[RFC3775](#)]. Routing Header issues were later documented in [[I-D.ietf-v6ops-security-overview](#)].

An eloquent and useful description of the operational security implications of RH0 was presented by Philippe Biondi and Arnaud Ebalard at the CanSecWest conference in Vancouver, 2007 [[CanSecWest07](#)]. This presentation resulted in widespread publicity

Abley, et al.

Expires November 17, 2007

[Page 4]

Internet-Draft

Deprecation of RH0

May 2007

for the risks associated with RH0.

This document also benefits from the contributions of IPv6 and V6OPS working group participants, including Jari Arkko, Arnaud Ebalard, Tim Enos, Brian Haberman, Jun-ichiro itojun HAGINO, Bob Hinden, JINMEI Tatuya, David Malone, Jeroen Massar, Dave Thaler and Guillaume Valadon.

8. References

8.1. Normative References

[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.

8.2. Informative References

[CanSecWest07]

BIONDI, P. and A. EBALARD, "IPv6 Routing Header Security", April 2007.

http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf

[I-D.ietf-v6ops-security-overview]

Davies, E., "IPv6 Transition/Co-existence Security Considerations", [draft-ietf-v6ops-security-overview-06](#) (work in progress), October 2006.

[I-D.savola-ipv6-rh-ha-security]

Savola, P., "Security of IPv6 Routing Header and Home Address Options", [draft-savola-ipv6-rh-ha-security-02](#) (work in progress), March 2002.

[I-D.savola-ipv6-rh-hosts]

Savola, P., "Note about Routing Header Processing on IPv6 Hosts", [draft-savola-ipv6-rh-hosts-00](#) (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.

Abley, et al.

Expires November 17, 2007

[Page 5]

Internet-Draft

Deprecation of RH0

May 2007

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.

[Appendix A](#). Change History

This section to be removed prior to publication.

00 Strawman, [draft-jabley-ipv6-rh0-is-evil](#), circulated to provoke discussion.

01 Clarified [Section 3](#); presented more options in [Section 4](#); added Pekka and George as authors. This document version was not widely circulated.

00 Renamed, [draft-ietf-ipv6-deprecate-rh0](#), a candidate working group document.

Authors' Addresses

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

Pekka Savola
CSC/FUNET
Espoo,
Finland

Email: psavola@funet.fi

George Neville-Neil
Neville-Neil Consulting
2261 Market St. #239
San Francisco, CA 94114
USA

Email: gnn@neville-neil.com

Abley, et al.

Expires November 17, 2007

[Page 6]

Internet-Draft

Deprecation of RH0

May 2007

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).