Network Working Group
Internet-Draft
Updates: 2460, 4294
(if approved)
Intended status: Standards Track
Expires: December 28, 2007

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

June 26, 2007

Deprecation of Type 0 Routing Headers in IPv6
draft-ietf-ipv6-deprecate-rh0-01

Status of this Memo

Copyright Notice

Abstract

The functionality provided by IPv6's Type 0 Routing Header can be exploited in order to achieve traffic amplification over a remote path 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 light of this security concern.

Table of Contents

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.

A single RH0 may contain multiple intermediate node addresses, and the same address may be included more than once in the same RH0. This allows a packet to be constructed such that it will oscillate between two RH0-processing hosts or routers many times. This allows a stream of packets from an attacker to be amplified along the path between two remote routers, which could be used to cause congestion along arbitrary remote paths and hence act as a denial-of-service mechanism. 88-fold amplification has been demonstrated using this technique [CanSecWest07].

This attack is particularly serious in that it affects the entire path between the two exploited nodes, not only the nodes themselves or their local networks. Analogous functionality may be found in the IPv4 source route option, but the opportunities for abuse are greater with RH0 due to the ability to specify many more intermediate node addresses in each packet.

The severity of this threat is considered to be sufficient to warrant deprecation of RH0 entirely. A side-effect is that this also eliminates benign RH0 use-cases; however, such applications may be facilitated by future Routing Header specifications.

Potential problems with RH0 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 resulted in the modification of the Mobile IPv6 specification to use the type 2 Routing Header instead of RH0 [RFC3775]. Vishwas Manral identified various risks associated with RH0 in 2006 including the amplification attack; several of these vulnerabilities (together with other issues) were later documented in [I-D.ietf-v6ops-security-overview].

A treatment 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 for the risks associated with RH0.

This document updates [RFC2460] and [RFC4294].

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

IPv6 nodes MUST NOT process RH0 in packets whose destination address in the IPv6 header is an address assigned 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, namely:

> If Segments Left is zero, the node must ignore the Routing header and proceed to process the next header in the packet, whose type is identified by the Next Header field in the Routing header.
>
> If Segments Left is non-zero, the node must discard the packet and send an ICMP Parameter Problem, Code 0, message to the packet's Source Address, pointing to the unrecognised Routing Type.

IPv6 implementations are no longer required to implement RH0 in any way.

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].

A site security policy intended to protect against attacks using RH0 SHOULD include the implementation of ingress filtering at the site border.

4.2. Firewall Policy

Blocking all IPv6 packets which carry Routing Headers (rather than specifically blocking type 0, and permitting other types) has very serious implications for the future development of IPv6. If even a small percentage of deployed firewalls block other types of routing headers by default, it will become impossible in practice to extend IPv6 routing headers. For example, Mobile IPv6 [RFC3775] relies upon a type-2 RH; wide-scale, indescriminate blocking of Routing Headers will make Mobile IPv6 undeployable.

Firewall policy intended to protect against packets containing RH0 MUST NOT simply filter all traffic with a routing header; it must be possible to disable forwarding of type 0 traffic without blocking other types of routing headers. In addition, the default configuration MUST permit forwarding of traffic using a RH other than 0.

5. Security Considerations

The purpose of this document is to deprecate a feature of IPv6 which has been shown to have undesirable security implications. Specific examples of vulnerabilities which are facilitated by the availability of RH0 can be found in [CanSecWest07]. In particular, RH0 provides a mechanism for traffic amplification, which might be used as a denial-of-service attack. A description of this functionality can be found in Section 1.

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. Acknowlegements

This document benefits from the contributions of many IPV6 and V6OPS working group participants, including Jari Arkko, Arnaud Ebalard, Tim Enos, Brian Haberman, Jun-ichiro itojun HAGINO, Bob Hinden, Thomas Narten, 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.

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

8.2. Informative References

[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

[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.

[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.

01-candidate-00 Incorporated text summarising some of the unwelcome uses of RH0; added some clariying text describing deprecation; modified some ambiguous text in Section 4.2; added "Updates: 4294".

01-candidate-01 Incorporated contributions from working group: substantially reduced Section 5; clarified wording in Section 3.

01-candidate-02 Moved description of traffic amplification to Section 1, and inserted a corresponding cross-reference in Section 5. Strengthened the language in Section 4.2 along the lines suggested by Thomas Narten. Small typos corrected. Added a further sentence in Section 4.1 intended to act as further encouragement for operators to implement [RFC3704].

01 Minor wordsmithing; removed some subjective language; adopted "intermediate node" nomenclature instead of "waypoint"; shifted some history from Section 7 to Section 1.

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

Full Copyright Statement

Intellectual Property

Acknowledgment

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