Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-smith-6man-more-secure-rh-03
Updates: 5095, 8200 (if approved)
Published: 23 February 2022
Intended Status: Standards Track
Expires: 27 August 2022
Authors: M.R. Smith

More Secure IPv6 Routing Header Processing

Abstract

The original IPv6 Type 0 Routing Header has been deprecated due to the security risk of a packet forwarding loop being formed, by specifying a large sequence of alternating IPv6 node addresses to visit. This memo proposes a method to prevent these forwarding loops forming, allowing the IPv6 Type 0 Routing Header to be more securely and more safely used. The method may also be applicable to other unicast source routing scenarios.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 27 August 2022.

Table of Contents

1. Introduction

[RFC5095] deprecated the IPv6 Type 0 Routing Header as it could be used to create a traffic loop, by specifying a large sequence of alternating IPv6 node addresses to visit. This traffic loop could consume large amounts of network capacity, causing congestion, and possibly a network capacity denial of service attack. (The packets caught in the forwarding loop would eventually be dropped as their hop-count field will eventually reach zero.)

This memo specifies a method of preventing these traffic loops occurring, which allows the IPv6 Type 0 to be more securely and more safely used. This method may also be applicable to other unicast source routing scenarios.

2. The Fundamental Problem

The fundamental problem with the type 0 RH, and other source Routing Headers that support multiple routing hops in general, is that packets can be made to travel back towards where they've come from. This then facilitates the first step of a packet being able to enter a forwarding loop.

3. Solution

Packets need to be prevented from travelling back towards where they've come from, which then prevents a forwarding loop from being formed.

The problem of packets going back towards where they've come from exists in multicast, and has been solved by performing a Reverse Path Forwarding (RPF) check on a packet as part of the multicast forwarding procedure.

This RPF check ensures that a packet does not leave via the router in direction back towards the packet's source address. This direction back towards the packet's source may be via the packet's ingress interface, or a different egress interface back towards the packet's source in an asymmetric routing scenario.

This memo specifies that a Reverse Path Forwarding Check is peformed when processing the IPv6 Type 0 Routing Header to prevent the packet going back towards its source.

[RFC3704], although describing RPF checks to prevent source IP address spoofing, provides good descriptions of the RPF checking process.

4. Method

The following method is used to process IPv6 Type 0 Routing Headers while also preventing their packets from entering a forwarding loop.

1. Perform the Type 0 Routing Header processing algorithm as specified in [RFC2460], section 4.4. This will result in the packet's Type 0 Routing Header and Destination Address being updated to the next address specified in the routing header to visit.

2. Perform an RPF check against the updated packet.

3. If the packet is to now travel back towards its source, discard the packet, and generate an ICMPv6 Destination Unreachable, Routing Header RPF Check Failed error (specified below), sending it to the packet's source (address).

4. Otherwise, forward the packet to its new Destination Address.

Note that an implementation could perform the RPF check against the next address specified in the Type 0 Routing Header before updating the packet's Type 0 Routing Header and Destination Address field as a processing optimisation. If the RPF check fails in this case, the packet's Type 0 Routing Header and Destination Address will need to be updated so that it can then be correctly used as the message body for the ICMPv6 Destination Unreachable error message [RFC4443].

5. ICMPv6 Destination Unreachable, Routing Header RPF Check Failed

A new ICMPv6 Destination Unreachable error message is defined for a "Routing Header RPF Check Failed", Type 1, Code [IANA-TBD]. Processing of this error message is as per the general Destination Unreachable message processing specified in [RFC4443]. There is no special handling of this error message at the receiver.

6. Updates to RFC8200

This memo makes the reason for the IPv6 Type 0 Routing Header deprecation invalid. Consequently, [RFC8200] is updated to now specify the Type 0 Routing Header formerly specified in [RFC2460].

7. More General Applicability

The method of preventing a packet or a frame from travelling back towards its origin when being forwarded can be applied to any unicast source routing scenario where a forwarding loop is possible.

Examples of where it could be applied are the IPv6 Segment Routing Header [RFC8754], Segment Routing over MPLS [RFC8660], the IPv6 Compressed Rouing Header [CRH] and IPv4 [RFC0791].

8. Inspiration

The idea of using an RPF check to prevent forwarding loops when performing unicast source routing was inspired by using an RPF check to prevent forwarding loops in hop-by-hop forwarding through the network using an anycast IPv6 address [FFANYCAST]. In this scenario, a packet is forwarded towards the next closest instance of the anycast address in the network, excluding anycast address instances that are back towards the packet's source.

9. Security Considerations

This memo addresses the primary security issue that caused the Type 0 Routing Header to be deprecated.

This memo does not address other security issues related to routing headers and source routing, such as using a routing header to bypass a security policy enforcement device, or untrusted packets with routing headers entering a routing header trusting domain. Other mitigations to these security issues, such as source address filtering at ingress to the local network, or packet authentication [RFC4302], need to be deployed.

10. IANA Considerations

IANA are requested to allocate a suitable Type 1 Destination Unreachable error code for "Routing Header RPF Check Failed".

11. Acknowledgements

Review and comments were provided by YOUR NAME HERE!

This memo was prepared using the xml2rfc tool.

12. Change Log [RFC Editor please remove]

draft-smith-6man-more-secure-rh-00, initial version, 2022-02-14

draft-smith-6man-more-secure-rh-01, 2022-02-17

- *IEEE 802.2 Source Route Bridging does a check for a forwarding loop when forwarding.

- *Better wording and minor corrections.

draft-smith-6man-more-secure-rh-02, 2022-02-24

- *Hop-by-hop anycast inspiration

draft-smith-6man-more-secure-rh-03, 2022-02-24

- *Extra greater than sign

13. References

13.1. Normative References

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <https://www.rfc-editor.org/info/rfc2460>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

13.2. Informative References

[CRH] "The IPv6 Compact Routing Header (CRH)", <https://datatracker.ietf.org/doc/draft-bonica-6man-comp-rtg-hdr/>.

[FFANYCAST] "IPv6 Formal Anycast Addresses and Functional Anycast Addresses", <https://datatracker.ietf.org/doc/draft-smith-6man-form-func-anycast-addresses/>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March 2004, <https://www.rfc-editor.org/info/rfc3704>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, DOI 10.17487/RFC5095, December 2007, <https://www.rfc-editor.org/info/rfc5095>.

[RFC8660] Bashandy, A., Ed., Filsfils, C., Ed., Previdi, S., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing with the MPLS Data Plane", RFC 8660, DOI 10.17487/RFC8660, December 2019, <https://www.rfc-editor.org/info/rfc8660>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.

Author's Address

Mark Smith
PO BOX 521
HEIDELBERG VIC 3084
Australia

Email: markzzzsmith@gmail.com