Deprecation of Source Routing Options in IPv4
draft-reitzel-ipv4-source-routing-is-evil-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/1id-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 March 1, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

[RFC0791] defines two IPv4 options called "Strict Source Routing" and "Loose Source Routing". Functionality provided by these options 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 RFC 791 to deprecate the use of the IPv4 Strict Source Routing Option as well as the IPv4 Loose Source Routing Option.
Table of Contents

1. Conventions Used In This Document .......................... 3
2. Introduction ....................................................... 3
3. Implementation ..................................................... 3
4. Operations ......................................................... 3
5. Security Considerations .......................................... 3
6. IANA Considerations .............................................. 4
7. Acknowledgements .................................................. 4
8. References .......................................................... 4
   8.1. Normative References ......................................... 4
   8.2. Informative References ....................................... 4
Author’s Address ...................................................... 4
Intellectual Property and Copyright Statements ................. 6
1. Conventions Used In This Document

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].

2. Introduction

[RFC0791] defines two IPv4 options called "Strict Source Routing" and "Loose Source Routing". Functionality provided by these options 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 RFC 791 to deprecate the use of the IPv4 Strict Source Routing Option as well as the IPv4 Loose Source Routing Option.

3. Implementation

Compliant IPv4 hosts and routers MUST NOT transmit IPv4 datagrams containing either the Strict Source Routing Option or the Loose Source Routing Option.

4. Operations

Compliant IPv4 hosts and routers that receive IPv4 datagrams containing either the Strict Source Routing or Loose Source Routing Options MUST silently discard those datagrams without further processing.

5. Security Considerations

The purpose of this document is to deprecate an IPv4 feature which has been shown to have serious security implications. These security implications have been well understood in the operator community for many years. For this reason, Internet Service Providers typically block all incoming IPv4 datagrams that include either the Strict Source Routing or Loose Source Routing Options.

Recently, researchers [BiondiEbalard] have demonstrated security vulnerabilities associated with the IPv6 Route Header Type 0 Extension. Because of its similar function, vulnerabilities associated with the IPv6 Route Header Type 0 Extension can be generalized to affect the above mentioned IPv4 options.
6. IANA Considerations

This document requests that IANA update the description of IPv4 Strict Source Routing and Loose Source Routing Options to indicate that the use of these options is deprecated.

7. Acknowledgements

This document follows in the spirit of [I-D.jabley-ipv6-rh0-is-evil], which proposes the deprecation of the IPv6 Route Header Type 0 Extension.

A description of security vulnerabilities associated with the the IPv6 Route Header Type 0 Extension was presented by Philippe Biondi and Arnaud Ebalard at the CanSecWest conference in Vancouver, 2007 [BiondiEbalard].

8. References

8.1. Normative References


8.2. Informative References

[BiondiEbalard]

[I-D.jabley-ipv6-rh0-is-evil]
Abley, J., "Deprecation of Type 0 Routing Headers in IPv6", draft-jabley-ipv6-rh0-is-evil-00 (work in progress), May 2007.
Author’s Address

Andrea M. Reitzel
Verizon Business
22001 Loudoun County Pkwy
Ashburn, VA  20147
US

Email: andrea.reitzel@verizonbusiness.com