

Routing Area Working Group

Internet Draft

Intended status: BCP

Expires: April 2009

R. Rahman
D. Ward
Cisco Systems
October 2008

Use of IP Router Alert Considered Dangerous
draft-rahman-rtg-router-alert-dangerous-00.txt

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 April 17, 2009.

Abstract

This document provides guidelines to address security concerns which arise with the use of IP Router Alert option [[RFC2113](#)] and [[RFC2711](#)]. RSVP, [[RFC2205](#)] and [[RFC3209](#)], and IGMP [[RFC3376](#)] are some of the protocols which make use of the IP Router Alert option. IP datagrams carrying the Router Alert option are usually examined in a router's "slow path" and an excess of such datagrams can cause performance degradation or packet drops in a router's "slow path".

Internet-Draft [draft-rahman-rtg-router-alert-dangerous-00.txt](#) October 2008

Table of Contents

1.	Introduction.....	2
2.	Conventions used in this document.....	2
3.	Security Risk Of IP Router Alert Option.....	2
4.	Guidelines For Use Of IP Router Alert Option.....	3
5.	Security Considerations.....	3
6.	IANA Considerations.....	4
7.	Conclusions.....	4
8.	Acknowledgments.....	4
9.	References.....	5
9.1.	Normative References.....	5

[1.](#) Introduction

The main purpose of this document is to describe the security risks associated with the use of IP Router Alert and to discourage new applications and protocols from using IP Router Alert.

[2.](#) 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 [RFC-2119](#) [[1](#)].

[3.](#) Security Risk Of IP Router Alert Option

IP datagrams carrying the Router Alert option are usually examined in a router's "slow path" and an excess of such datagrams can cause performance degradation or packet drops in a router's "slow path".

[RFC4081] and [[RFC2711](#)] mention the security risks associated with the use of the IP Router Alert option: flooding a router with bogus IP datagrams which contain the IP Router Alert option would cause a performance degradation of the router's "slow path" and can also lead to packet drops in the "slow path".

[RFC2711] mentions that limiting, by rate or some other means, the use of Router Alert option is a way of protecting against a potential attack. If rate limiting is used as a protection mechanism and the

granularity of the rate limiting is coarse, an attack using packet types of one protocol could severely degrade the operation of other protocols using IP Router Alert option.

Internet-Draft [draft-rahman-rtg-router-alert-dangerous-00.txt](#) October 2008

[4.](#) Guidelines For Use Of IP Router Alert Option

To protect the "slow path" against DOS attacks, a router MUST have a means of limiting the number of Router Alert IP datagrams which go to the "slow path".

If there are multiple protocols which make use of IP Router Alert option on a router, the limiting MUST be able to distinguish between the various protocols. E.g. if rate limiting is used, there MUST be different rate limit pools for the protocols so that an attack on one protocol will not affect the operation of another protocol.

IP Router Alert packets MUST NOT be sent to the "slow path" unless there is at least one protocol enabled which uses the IP Router Alert option.

A router SHOULD inspect Router Alert packets before sending them to the "slow path" so that if the protocol to which a packet belongs is not enabled on the router or on the incoming interface (physical or virtual), then the packet is dropped.

Introducing new protocols/applications which make use of IP Router Alert option MUST not provide a means of attacking or harming deployed protocols such as RSVP and IGMP which already make use of the IP Router Alert option.

Routing and signaling users of IP Router Alert, e.g. IGMP and RSVP, are the highest priority users and MUST NOT be impacted by other users of IP Router Alert.

Any application that relies on IP Router Alert should expect that the incoming packets MAY be dropped by default and that a special filter is needed to let the packets through.

All non-routing and non-signaling IP Router Alert packets, when enabled, may be significantly rate limited.

Creating an application or protocol that uses IP Router Alert is considered harmful and is strongly discouraged. A different mechanism should be used to decrease the risk of impacting existing routing and signaling protocols which use IP Router Alert

[5.](#) Security Considerations

This document provides guidelines for security risks which are present with the use of IP Router Alert option. Its purpose is to

<Rahman>

Expires April 17, 2009

[Page 3]

Internet-Draft [draft-rahman-rtg-router-alert-dangerous-00.txt](#) October 2008

have greater security against DDOS attacks and to discourage new applications from using IP Router Alert since this would cause a security risk against current users of IP Router Alert.

[6.](#) IANA Considerations

[7.](#) Conclusions

Use of IP Router Alert is a security risk and should be discouraged for new applications and protocols.

[8.](#) Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Internet-Draft [draft-rahman-rtg-router-alert-dangerous-00.txt](#) October 2008

9. References

- [RFC2113] "IP Router Alert Option", [RFC 2113](#), D. Katz, February 1997.
- [[RFC2711](#)] "IPv6 Router Alert Option", [RFC 2711](#), C. Partridge, et al, October 1999.
- [[RFC2205](#)] "Resource ReSerVation Protocol (RSVP) - Version 1, Functional Specification", [RFC 2205](#), Braden, et al, September 1997.
- [[RFC3209](#)] "Extensions to RSVP for LSP Tunnels", D. Awduche, et al, [RFC 3209](#), December 2001.
- [[RFC3376](#)] "Internet Group Management Protocol, Version 3", [RFC 3376](#), B. Cain, et al, October 2002.
- [[RFC4081](#)] "Security Threats For Next Steps in Signaling (NSIS)", [RFC 4081](#), H. Tschofenig, et al, June 2005

9.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
 - [2] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](#), Internet Mail Consortium and Demon Internet Ltd., November 1997.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC2234] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](#), Internet Mail Consortium and Demon Internet Ltd., November 1997.

Author's Addresses

Reshad Rahman
Cisco Systems Inc.
2000 Innovation Dr.,
Kanata, Ontario, K2K 3E8
Canada.
Phone: (613)-254-3519
Email: rrahman@cisco.com

David Ward
Cisco Systems Inc.
3750 Cisco Way,

<Rahman>

Expires April 17, 2009

[Page 5]

Internet-Draft [draft-rahman-rtg-router-alert-dangerous-00.txt](#) October 2008

San Jose, California, 95134
United States
Phone: (651)-726-2368
Email: wardd@cisco.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

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 Statement

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.