

December 19, 2013

Mitigation against IPv6 Router Advertisements flooding
[draft-moonesamy-ra-flood-limit-01](#)

Abstract

An IPv6 Router Advertisements flooding attack can cause a node to consume all CPU resources available making the system unusable and unresponsive. This document recommends some configurable variables as a mitigation against an IPv6 Router Advertisements flooding attack.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [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/1id-abstracts.html>

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

Copyright and License Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Router Advertisement Configuration Variables	3
2.1	MaxInterfacePrefixes	3
2.2	MaxInterfaceRouters	3
2.3	MaxRedirect	3
3.	Security Considerations	3
4.	IANA Considerations	4
5.	Acknowledgments	4
6.	References	4
6.1	Normative References	4
6.2	Informative References	4
Appendix A	4
Authors' Addresses	4

1. Introduction

The Neighbor Discovery protocol [[RFC4861](#)] describes the operation of IPv6 Router Advertisements (RAs) that are used to determine node configuration information during the IPv6 autoconfiguration process. A Router Advertisements flooding attack [[RAFLOOD](#)] can cause a node to consume all CPU resources available or cause kernel memory exhaustion making the system unusable and unresponsive. The problem with rogue IPv6 Router Advertisement is documented in [RFC 6104](#) [[RFC6104](#)].

This document recommends some configurable variables as a mitigation against a Router Advertisements flooding attack.

2. Router Advertisement Configuration Variables

A host will silently discard a Router Advertisement once the configurable limit is reached. Default values are specified to make it unnecessary to configure any of these variables.

2.1 MaxInterfacePrefixes

This variable is the maximum number of prefixes created per interface by Router Advertisements.

Default: 16

2.2. MaxInterfaceRouters

This variable is the maximum number of default routers created per interface by Route Advertisements.

Default: 16

2.3. MaxRedirect

This variable is the maximum number of dynamic routes created via ICMPv6 Redirect messages.

Default: 4096

3. Security Considerations

The Router Advertisements flooding attack can cause a denial-of-service. The configuration variables described in this document can be used to limit the scope of the attack. There is a high probability that valid Router Advertisement information may be lost even with the mitigation described in this document. It is

recommended to log a system alert about the configurable limit reached.

4. IANA Considerations

[RFC Editor: please remove this section]

5. Acknowledgments

Marc Heuse published an advisory about the IPv6 Router Advertisements flooding attack in 2011. The authors would like to thank David Farmer, Joel M. Halpern, Marc Heuse and Arturo Servin for contributing to the document.

6. References

6.1. Normative References

[RFC4861] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 2461](#), December 1998.

6.2. Informative References

[RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", [RFC 6104](#), February 2011.

[RAFLOOD] <http://www.mh-sec.de/downloads/mh-RA_flooding_CVE-2010-multiple.txt>

Appendix A

The default values mentioned in [Section 2](#) have been implemented in FreeBSD, NetBSD and OpenBSD.

Authors' Addresses

S. Moonesamy
76, Ylang Ylang Avenue
Quatres Bornes
Mauritius

Email: sm+ietf@elandsys.com

