

IPv6 Operations Working Group (v6ops)
Internet-Draft
Intended status: Informational
Expires: December 2, 2011

F. Gont
UK CPNI
May 31, 2011

IPv6 Router Advertisement Guard (RA-Guard) Evasion
draft-gont-v6ops-ra-guard-evasion-00

Abstract

The IPv6 Router Advertisement Guard (RA-Guard) mechanism is commonly employed to mitigate attack vectors based on forged ICMPv6 Router Advertisement messages. Many existing IPv6 deployments rely on RA-Guard as the first line of defense against the aforementioned attack vectors. This document describes possible ways in which current RA-Guard implementations can be circumvented, and discusses possible mitigations.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

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 <http://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 December 2, 2011.

Copyright Notice

Copyright (c) 2011 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 Guard (RA Guard) Evasion Vulnerability .	4
2.1.	Attack Vector based on IPv6 Extension Headers	4
2.2.	Attack vector based on IPv6 fragmentation	4
3.	Mitigations	8
4.	Other Implications	9
5.	Security Considerations	10
6.	Acknowledgements	11
7.	References	12
7.1.	Normative References	12
7.2.	Informative References	12
Appendix A.	Assessment tools	13
	Author's Address	14

1. Introduction

IPv6 Router Advertisement Guard (RA-Guard) is a mitigation technique for attack vectors based on ICMPv6 Router Advertisement messages. describes the problem statement of "Rogue IPv6 Router Advertisements", and specifies the "IPv6 Router Advertisement Guard" functionality.

The basic concept behind RA-Guard is that a layer-2 device filters ICMPv6 Router Advertisement messages, according to a number of different criteria. The most basic filtering criteria is that Router Advertisement messages are discarded by the layer-2 device unless they are received on a specified port of the layer-2 device. Clearly, the effectiveness of the RA Guard mitigation relies on the ability of the layer-2 device of identifying ICMPv6 Router Advertisement messages.

As part of the project "Security Assessment of the Internet Protocol version 6 (IPv6)" [[CPNI-IPv6](#)], we devised a number of techniques for circumventing the RA-Guard protection, which are described in the following sections of this document. These techniques, and the corresponding tools to assess their effectiveness, had so far been made available only to vendors, in the hopes that they could implement counter-measures before they were publicly disclosed. However, since there has been some public discussion about these issues, it was deemed as appropriate to publish the present document.

It should be noted that the aforementioned techniques could also be exploited to evade network monitoring tools such as NDPMon [[NDPMon](#)], ramond [[ramond](#)], and rafixd [[rafixd](#)].

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](#) [[RFC2119](#)].

2. Router Advertisement Guard (RA Guard) Evasion Vulnerability

The following subsections describe two different vectors for evading the RA-Guard protection. [Section 2.1](#) describes an attack vector based on the use of IPv6 Extension Headers with the ICMPv6 Router Advertisement messages, which may be used to circumvent the RA-Guard protection of those implementations that fail to process an entire IPv6 header chain when trying to identify the ICMPv6 Router Advertisement messages. [Section 2.2](#) describes an attack method based on the use of IPv6 fragmentation, possibly in conjunction with the use of IPv6 Extension Headers. This later vector is expected to be effective with all existing implementations of the RA-Guard functionality.

2.1. Attack Vector based on IPv6 Extension Headers

While there is currently no legitimate for IPv6 Extension Headers in ICMPv6 Router Advertisement messages, implementations allow the use of Extension Headers included in these messages, by simple ignoring the received options. We believe that some implementations may simply try to identify ICMPv6 Router Advertisement messages by looking at the "Next Header" field of the fixed IPv6 header, rather than following the entire header chain. As a result, these implementations would fail to identify any ICMPv6 Router Advertisement messages that include any Extension Headers (for example, Hop by Hop Options header, Destination Options Header, etc.).

The following figure illustrates the structure of ICMPv6 Router Advertisement messages that implements this RA-Guard evasion technique:

```

+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|NH=60|      |NH=58|      |      |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| IPv6 header | Dst Opt Hdr | ICMPv6 Router Advertisement |
+              +              +
|              |              |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

2.2. Attack vector based on IPv6 fragmentation

While the attack vector described in [Section 2.1](#) may be effective with implementations that fail to process the entire header chain, it can easily be mitigated by an RA-Guard implementation, since all the information needed to identify ICMPv6 Router Advertisement messages is present in the attack packets.

Gont

Expires December 2, 2011

[Page 4]

This section presents a different attack vector, which aims at making it virtually impossible for a layer-2 device to identify ICMPv6 Router Advertisements by leveraging the IPv6 Fragment Header. The basic idea behind this attack vector is that if the forged ICMPv6 Router Advertisement is fragmented into at least two fragments, the layer-2 device implementing "RA-Guard" would be unable to identify the attack packet, and would those would fail do block it.

A first variant of this attack vector would be an original ICMPv6 Router Advertisement message preceded with a Destination Options Header, that results in two fragments. The following figure illustrates the "original" attack packet, prior to fragmentation, and the two resulting fragments which are actually sent as part of the attack.

Original packet:

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|NH=60|          |NH=58|          |          |          |
+---+---+      +---+---+          +          +
| IPv6 header |          Dst Opt Hdr          | ICMPv6 RA |
+          +          +          +
|          |          |          |          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

First fragment:

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|NH=44|          |NH=60|          |NH=58|          |
+---+---+      +---+---+      +---+---+          +
| IPv6 Header |      Frag Hdr |          Dst Opt Hdr          |
+          +          +          +
|          |          |          |          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Second fragment:

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|NH=44|          |NH=60|          |          |          |
+---+---+      +---+---+      +          +          +
| IPv6 header |      Frag Hdr | Dst Opt Hdr | ICMPv6 RA |
+          +          +          +          +
|          |          |          |          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

In this variant, by leveraging the use of the Fragment Header

together with the use of the Destination Options header, the attacker is able to conceal the type of ICMPv6 error message he is sending. Unless the layer-2 device were to implement IPv6 fragment reassembly, it would be impossible for the device to identify the ICMPv6 type of the message.

It is possible to take this idea further, such that it is also impossible for the layer-2 device to detect that the attacker is sending an ICMPv6 message in the first place. This can be achieved with an original ICMPv6 Router Advertisement message preceded with two Destination Options Headers, that results in two fragments. The following figure illustrates the "original" attack packet, prior to fragmentation, and the two resulting packets which are actually sent as part of the attack.

Original packet:

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|NH=60|          |NH=60|          |NH=58|          |          |
+---+---+      +---+---+      +---+---+      +          +
| IPv6 header  | Dst Opt Hdr | Dst Opt Hdr | ICMPv6 RA |
+          +          +          +          +
|          |          |          |          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

First fragment:

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|NH=44|          |NH=60|          |NH=58|          |          |
+---+---+      +---+---+      +---+---+      +          +
| IPv6 header  | Frag Hdr  |          Dst Opt Hdr          |
+          +          +          +          +
|          |          |          |          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Second fragment:

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|NH=44|          |NH=60|          |          |NH=58|          |          |
+---+---+      +---+---+      +          +---+---+      +          +
| IPv6 header  | Frag Hdr  | Dst O Hdr | Dst Opt Hdr | ICMPv6 RA |
+          +          +          +          +          +
|          |          |          |          |          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

It should be obvious that even if the layer-2 device tried to follow the entire IPv6 header chain, it would still be unable to identify

that the fragments above transport an ICMPv6 message.

3. Mitigations

The most effective and efficient mitigation for the RA-Guard evasion vulnerability discussed in this document would be to prohibit the use of IPv6 Extension Headers in Neighbor Discovery messages, as proposed in [[draft-gont-6man-nd-extension-headers](#)].

Nevertheless, an administrator might want to mitigate these vulnerabilities by deploying more advanced filtering. The following filtering rules could be implemented as part of an "RA-Guard" implementation, such that the vulnerabilities discussed in this document can be mitigated:

- o When trying to identify an ICMPv6 Router Advertisement message, follow the IPv6 header chain, enforcing a limit on the maximum number of Extension Headers that is allowed for each packet. If such limit is exceeded, block the packet.
- o If the layer-2 device is unable to identify whether the packet is an ICMPv6 Router Advertisement message or not (i.e., the packet is a fragment, and the necessary information is missing), then, if the IPv6 Source Address of the packet is a link-local address, block the packet.
- o In all other cases, pass the packet as usual.

This filtering policy assumes that host implementations require that the IPv6 Source Address of ICMPv6 Router Advertisement messages be a link-local address, and that they discard the packet if this check fails, as required by the current IETF specifications [[RFC4861](#)]. Unfortunately, it should be noted that the aforementioned filtering policy might be inefficient to implement (if at all possible), and might also result (at least in theory) in false positives.

4. Other Implications

A similar concept to that of "RA-Guard" has been implemented for protecting against forged DHCPv6 messages. Such protection can be circumvented with the same techniques discussed in this document, and the counter-measures for such evasion attack are analogous to those described in [Section 3](#) of this document.

5. Security Considerations

This document describes a number of techniques to circumvent a mechanism known as "RA-Guard", which many organizations deploy as a "first line of defense" against attacks based on forged Router Advertisements.

The most effective and efficient mitigation for these attacks would be to prohibit the use of IPv6 extension headers (as proposed by [\[draft-gont-6man-nd-extension-headers\]](#)), such that the RA-Guard protection cannot be easily circumvented. However, since this mitigation requires an update to existing implementations, in the short term some network administrators might want to mitigate these issues by implemented the more advanced filtering policy described in [Section 3](#).

6. Acknowledgements

This document resulted from the project "Security Assessment of the Internet Protocol version 6 (IPv6)" [[CPNI-IPv6](#)], carried out by Fernando Gont on behalf of the UK Centre for the Protection of National Infrastructure (CPNI). The author would like to thank the UK CPNI, for their continued support.

7. References

7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.

7.2. Informative References

- [RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", [RFC 6104](#), February 2011.
- [RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", [RFC 6105](#), February 2011.
- [[draft-gont-6man-nd-extension-headers](#)]
Gont, F., "Security Implications of the Use of IPv6 Extension Headers with IPv6 Neighbor Discovery", IETF Internet Draft, [draft-gont-6man-nd-extension-headers](#), work in progress, May 2011.
- [CPNI-IPv6]
Gont, F., "Security Assessment of the Internet Protocol version 6 (IPv6)", UK Centre for the Protection of National Infrastructure, (to be published).
- [NDPMon] "NDPMon - IPv6 Neighbor Discovery Protocol Monitor", <<http://ndpmon.sourceforge.net/>>.
- [rafixd] "rafixd", <<http://www.kame.net/dev/cvsweb2.cgi/kame/kame/kame/rafixd/>>.
- [ramond] "ramond", <<http://ramond.sourceforge.net/>>.
- [THC-IPv6]
"THC-IPv6", <<http://www.thc.org/thc-ipv6/>>.

[Appendix A](#). Assessment tools

CPNI has produced assessment tools, which have not yet been made publicly available. If you think that you would benefit from these tools to assess the security of your network or of your RA-Guard implementation, we might be able to provide a copy of the tools (please contact Fernando Gont at fernando@gont.com.ar).

[THC-IPV6] is a publicly-available set of tools that implements some of the techniques described in this document.

Author's Address

Fernando Gont
Centre for the Protection of National Infrastructure

Email: fernando@gont.com.ar

URI: <http://www.gont.com.ar>