IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 2460 (if approved)
Intended status: Standards Track
Expires: June 16, 2012

F. Gont
UK CPNI

December 14, 2011

Security Implications of IPv6 options of Type 10xxxxxx
draft-gont-6man-ipv6-smurf-amplifier-00

Abstract

When an IPv6 node processing an IPv6 packet does not support an IPv6 option whose two-highest-order bits of the Option Type are '10', it is required to respond with an ICMPv6 Parameter Problem error message, even if the Destination Address of the packet was a multicast address. This feature provides an amplification vector, opening the door to an IPv6 version of the 'Smurf' Denial-of-Service (DoS) attack found in IPv4 networks. This document discusses the security implications of the aforementioned options, and formally updates RFC 2460 such that this attack vector is eliminated. Additionally, it describes a number of operational mitigations that could be deployed against this attack vector.

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 This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.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 June 16, 2012.

Copyright Notice

Table of Contents

1. Introduction

As described in Section 4.2 of [RFC2460], when a node processing an IPv6 packet does not support an IPv6 option whose two-highest-order bits of the Option Type are '10', it should respond with an ICMPv6 Parameter Problem error message, even if the Destination Address of the packet was a multicast address. This feature provides an amplification vector, opening the door to an IPv6 version of the 'Smurf' Denial-of-Service (DoS) attack [CERT1998] [RFC6274] found in IPv4 networks.

An attacker could exploit the aforementioned amplification vector by sending forged IPv6 packets with the IPv6 address of the victim system as the Source Address of his packets, a multicast address as the Destination Address, and an unsupported option (with an Option Type of '10xxxxxx') in a Destination Options Header. Upon receipt of the forged packet, each processing node would respond with an ICMPv6 Parameter Problem, code 2, error message, pointing to the unsupported option type. Thus, the systems belonging to the multicast group specified by the multicast address contained in the Destination Address field would serve as an 'amplifier network'.

> It should be noted that if the multicast RPF check is used (e.g. to prevent routing loops), this would prevent an attacker from forging the Source Address of a packet to an arbitrary value, thus preventing an attacker from launching this attack against a remote network.
>
> Chapter 5 of [Juniper2010] discusses multicast RPF configuration for Juniper routers.

Section 2.1 updates RFC 2460 [RFC2460], such that the aforementioned attack vector is eliminated. Section 2.2 describes a number of operational mitigations for the aforementioned attack vector.

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. Proposed countermeasures

2.1. Updating RFC 2460

Considering the security implications discussed in Section 1, and since there are no known legitimate uses of IPv6 options of type '10xxxxxx', this document updates RFC 2460 [RFC2460] as follows:

A node that receives a packet containing an unsupported IPv6 option of type '10xxxxxx', MUST process the packet as if the two-highest-order bits of the option were '11'. That is, the packet should be dropped, and an ICMPv6 Parameter Problem error message should be sent to the Source Address of the packet subject to the ICMPv6 error sending rules specified in [RFC4443] (which means that no ICMPv6 error message must be sent if the Destination Address of the offending packet is a multicast address).

2.2. Operational mitigations

This section describes a number of operational mitigations that could be implemented for the aforementioned attack vector:

- Firstly, IPv6 nodes should limit their ICMPv6 traffic. This is a general mitigation technique for any bandwidth-exhaustion attack that relies on ICMPv6 traffic. This could be enforced at the hosts themselves, or at any router connecting such hosts to the public network.

- Secondly, as noted in Section 1 of this document, the multicast

RPF check enabled such that an attacker cannot forge the Source Address of a packet to an arbitrary value, thus preventing an attacker from launching this attack against a remote network.

3. IANA Considerations

There are no IANA registries within this document. The RFC-Editor can remove this section before publication of this document as an RFC.

4. Security Considerations

This document describes how IPv6 options whose two-highest-order bits of the Option Type are '10' could possibly be exploited to perform an IPv6 version of the 'Smurf' Denial-of-Service (DoS) attack [CERT1998] [RFC6274] found in IPv4 networks. It formally updates RFC 2460 [RFC2460] such that this attack vector is eliminated., and also describes a number of operational mitigations that could be deployed against this attack vector.

5. Acknowledgements

This document is based on the technical report "Security Assessment of the Internet Protocol version 6 (IPv6)" [CPNI-IPv6] authored by Fernando Gont on behalf of the UK Centre for the Protection of National Infrastructure (CPNI).

Fernando Gont would like to thank CPNI (http://www.cpni.gov.uk) for

their continued support.

6. References

6.1. Normative References

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

6.2. Informative References

[RFC6274] Gont, F., "Security Assessment of the Internet Protocol Version 4", RFC 6274, July 2011.

[CPNI-IPv6] Gont, F., "Security Assessment of the Internet Protocol version 6 (IPv6)", UK Centre for the Protection of National Infrastructure, (available on request).

[CERT1998] CERT, "CERT Advisory CA-1998-01: Smurf IP Denial-of-Service Attacks", 1998, <http://www.cert.org/advisories/CA-1998-01.html>.

[Juniper2010] Juniper, "JunosE Software for E Series Broadband Services Routers Multicast Routing Configuration Guide", 2010, <http://www.juniper.net/techpubs/en_US/junose11.2/information-products/topic-collections/swconfig-multicast-routing/book-swconfig-multicast.pdf>.

Author's Address

Fernando Gont
UK CPNI

Email: fgont@si6networks.com
URI: http://www.cpni.gov.uk