IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 2460, 4443 (if approved)
Intended status: Standards Track
Expires: September 22, 2013

F. Gont
SI6 Networks / UTN-FRH
W. Liu
Huawei Technologies
March 21, 2013

Security Implications of IPv6 Options of Type 10xxxxxx
draft-gont-6man-ipv6-smurf-amplifier-03

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 and RFC 4443 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

Copyright Notice

Table of Contents

1. Introduction

IPv6 has eliminated most of the amplification vectors that were available in IPv4 to perform 'Smurf'-like Denial of Service (DoS) attacks [CERT1998]. However, an amplification vector has been left in the core IPv6 and ICMPv6 specifications ([RFC2460] and [RFC4443]) that would allow for an IPv6 version of the 'Smurf' Denial-of-Service (DoS) attacks [CERT1998] [RFC6274] found in IPv4 networks. The aforementioned vector is based on the use of unsupported IPv6 options, used in combination with multicast destinations.

[RFC2460] specifies, in Section 4.2, that 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. [RFC4443] specifies, in Section 2.4 (page 6), that packets destined to an IPv6 multicast address should not elicit ICMPv6 error messages, with the exception of ICMPv6 Packet Too Big messages (such that Path-MTU Discovery works for IPv6 multicast) and the Parameter Problem Message, Code 2 for reporting an unrecognized IPv6 option that has the Option Type highest-order two bits set to 10.

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 receiving host 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 updates RFC 2460 [RFC2460] and RFC 4443 [RFC4443], such that the aforementioned attack vector is eliminated. Section 3 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. Updating RFC 2460 and RFC 4443

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 the corresponding specifications to eliminate these issues.

The following text in Section 4.2 (page 9) of [RFC2460]:

> 10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

is replaced with:

> 10 - discard the packet and send an ICMP Parameter Problem, Code 2, message to the packet's Source Address (pointing to the unrecognized Option Type), only if (1) the packet's Destination Address was not a multicast address, or (2) the packet's Destination Address was a multicast address, but the node sending the Parameter Problem error message can assert that the Source Address of the packet eliciting the error message has not been forged.

Additionally, the following text in Section 2.4 (page 6) of [RFC4443]:

> (e.3) A packet destined to an IPv6 multicast address. (There are two exceptions to this rule: (1) the Packet Too Big Message (Section 3.2) to allow Path MTU discovery to work for IPv6 multicast, and (2) the Parameter Problem Message, Code 2 (Section 3.4) reporting an unrecognized IPv6 option (see Section 4.2 of [IPv6]) that has the Option Type highest-order two bits set to 10).

is replaced with:

(e.3) A packet destined to an IPv6 multicast address. (There is one exception to this rule: the Packet Too Big Message (Section 3.2) to allow Path MTU discovery to work for IPv6 multicast).

(e.3) A packet destined to an IPv6 multicast address. (There are two exceptions to this rule: (1) the Packet Too Big Message (Section 3.2) to allow Path MTU discovery to work for IPv6 multicast, and (2) the Parameter Problem Message, Code 2 (Section 3.4) reporting an unrecognized IPv6 option that has the Option Type highest-order two bits set to 10, *provided* the node sending the Parameter Problem message can assert that the Source Address of the packet eliciting the error message has not been forged.).

3. 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 could be 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.

4. 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.

5. Security Considerations

This document describes how IPv6 options whose two-highest-order bits of the Option Type are ’10’ could 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.

6. Acknowledgements

The authors would like to thank (in alphabetical order) Francis Dupont, Joel Halpern, Suresh Krishnan, Simon Perreault, Dave Thaler, and Ole Troan, for providing valuable comments on earlier versions of this document.

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.

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.

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

[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.

7.2. 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>.

Authors' Addresses

Fernando Gont
SI6 Networks / UTN-FRH
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: http://www.si6networks.com

Will (Shucheng) Liu
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: liushucheng@huawei.com