IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 2460 (if approved)
Intended status: Standards Track
Expires: December 31, 2012

F. Gont
SI6 Networks / UTN-FRH
V. Manral
Hewlett-Packard Corp.

June 29, 2012

Security and Interoperability Implications of Oversized IPv6 Header Chains
draft-ietf-6man-oversized-header-chain-00

Abstract

The IPv6 specification allows IPv6 header chains of an arbitrary size. The specification also allows options which can in turn extend each of the headers. In those scenarios in which the IPv6 header chain or options are unusually long and packets are fragmented, or scenarios in which the fragment size is very small, the first fragment of a packet may fail to include the entire IPv6 header chain. This document discusses the interoperability and security problems of such traffic, and updates RFC 2460 such that the first fragment of a packet is required to contain the entire IPv6 header chain.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

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 31, 2012.

Table of Contents

1. Introduction

[RFC2460] allows for an IPv6 header chain of an arbitrary size. It also allows the headers themselves to have options, which can change the size of the headers. In those scenarios in which the IPv6 header chain is unusually long and packets are fragmented, or scenarios in which the fragment size is very small, the first fragment of a packet may fail to include the entire IPv6 header chain. This document discusses the interoperability and security problems of such traffic, and updates RFC 2460 such that the first fragment of a fragmented datagram is required to contain the entire IPv6 header chain.

It should be noted that this requirement does not preclude the use of e.g. IPv6 jumbo payloads but instead merely requires that all *headers*, starting from IPv6 base header and continuing up to the upper layer header (e.g. TCP or the like) be present in the first fragment.

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. Interoperability Implications of Oversized IPv6 Header Chains

Some transition technologies, such as NAT64 [RFC6146], may need to have access to the entire IPv6 header chain in order to associate an incoming IPv6 packet with an ongoing "session".

> For instance, Section 3.4 of [RFC6146] states that "The NAT64 MAY require that the UDP, TCP, or ICMP header be completely contained within the fragment that contains fragment offset equal to zero".

Failure to include the entire IPv6 header chain in the first-fragment may cause the translation function to fail, with the corresponding packets being dropped.

3. Forwarding Implications of Oversized IPv6 Header Chains

A lot of the switches and Routers in the internet do hardware based forwarding. To be able to achieve a level of throughput, there is a fixed maximum number of clock cycles dedicated to each packet. However with the use of unlimited options and header interleaving, larger packets with a lot of interleaving have to be forwarded to the software. It is for this reason that the maximum size of valid packets with interleaved headers needs to be limited.

4. Security Implications of Oversized IPv6 Header Chains

Most firewalls enforce they filtering policy based on the following parameters:

- Source IP address
- Destination IP address
- Protocol type
- Source port number
- Destination port number

Some firewalls reassemble fragmented packets before applying a filtering policy, and thus always have the aforementioned information available when deciding whether to allow or block a packet. However, other stateless firewalls (generally prevalent on small/ home office equipment) do not reassemble fragmented traffic, and hence have to enforce their filtering policy based on the information contained in the received fragment, as opposed to the information contained in the reassembled datagram.

When presented with fragmented traffic, many of such firewalls typically enforce their policy only on the first fragment of a packet, based on the assumption that if the first fragment is dropped, reassembly of the corresponding datagram will fail, and thus such datagram will be effectively blocked. However, if the first fragment fails to include the entire IPv6 header chain, they may have no option other than "blindly" allowing or blocking the corresponding fragment. If they blindly allow the packet, then the firewall can be easily circumvented by intentionally sending fragmented packets that fail to include the entire IPv6 header chain in the first fragment. On the other hand, first-fragments that fail to include the entire IPv6 header chain have never been formally deprecated and thus, in theory, might be legitimately generated.

5. Updating RFC 2460

If a packet is fragmented, the first fragment of the packet (i.e., that with a Fragment Offset of 0) MUST contain the entire IPv6 header chain.

6. 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.

7. Security Considerations

This document describes the interoperability and security implications of IPv6 packets or first-fragments that fail to include the entire IPv6 header chain. The security implications include the possibility of an attacker evading network security controls such as firewalls and Network Intrusion Detection Systems (NIDS) [CPNI-IPv6].

This document updates RFC 2460 such that those packets are forbidden, thus preventing the aforementioned issues.

8. Acknowledgements

The authors would like to thank (in alphabetical order) Ran Atkinson and Dave Thaler for providing valuable comments on earlier versions of this document.

9. References

9.1. 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.

9.2. Informative References

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 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).

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

Vishwas Manral
Hewlett-Packard Corp.
191111 Pruneridge Ave.
Cupertino, CA 95014
US

Phone: 408-447-1497
Email: vishwas.manral@hp.com
URI: