Operational Security Capabilities for F. Gont
IP Network Infrastructure (opsec) SI6 Networks / UTN-FRH
Internet-Draft W. Liu
Intended status: BCP Huawei Technologies
Expires: June 15, 2013 G. Van de Velde
Cisco Systems
December 12, 2012

DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers
draft-ietf-opsec-dhcpv6-shield-00

Abstract

This document specifies a mechanism for protecting hosts connected to a broadcast network against rogue DHCPv6 servers. The aforementioned mechanism is based on DHCPv6 packet-filtering at the layer-2 device on which the packets are received. The aforementioned mechanism has been widely deployed in IPv4 networks ('DHCP snooping'), and hence it is desirable that similar functionality be provided for IPv6 networks.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document specifies a mechanism for protecting hosts connected to a broadcast network against rogue DHCPv6 servers [RFC3315]. This mechanism is analogous to the RA-Guard mechanism [RFC6104] [RFC6105] [I-D.ietf-v6ops-ra-guard-implementation] intended for protection against rogue Router Advertisement messages.

The basic concept behind DHCPv6-Shield is that a layer-2 device filters DHCPv6 messages meant to DHCPv6 clients, according to a number of different criteria. The most basic filtering criterion being that the aforementioned DHCPv6 messages are discarded by the layer-2 device unless they are received on a specified port of the layer-2 device.

Before the DCHPv6-Shield device is deployed, the administrator specifies the layer-2 port(s) on which DHCPv6 packets meant for DHCPv6 clients are allowed. Only those ports to which a DHCPv6 server is to be connected should be specified as such. Once deployed, the DHCPv6-Shield device inspects received packets, and allows (i.e. passes) DHCPv6 messages meant for DHCPv6 clients only if they are received on layer-2 ports that have been explicitly configured for such purpose.

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. DHCPv6-Shield Configuration

Before being deployed for production, the DHCPv6-Shield device MUST me configured with respect to which layer-2 ports are allowed to send DHCPv6 packets to DHCPv6 clients. Only those layer-2 ports explicitly configured for such purpose will be allowed to send DHCPv6 packets to DHCPv6 clients.

3. DHCPv6-Shield Implementation Advice

The following filtering rules MUST be enforced as part of an DHCPv6-Shield implementation on those ports that are not allowed to send DHCPv6 packets to DHCPv6 clients:

1. DHCPv6-Shield MUST parse the IPv6 entire header chain present in the packet, to identify whether it is a DHCPv6 packet meant for a DHCPv6 client.

   RATIONALE: [RFC6564] specifies a uniform format for IPv6 Extension Header, thus meaning that an IPv6 node can parse an IPv6 header chain even if it contains Extension Headers that are not currently supported by that node. Additionally, [I-D.ietf-6man-oversized-header-chain] requires that if a packet is fragmented, the first fragment contains the entire IPv6 header chain.

   DHCPv6-Shield implementations MUST NOT enforce a limit on the number of bytes they can inspect (starting from the beginning of the IPv6 packet), since this could introduce false-positives: legitimate packets could be dropped simply because the DHCPv6-Shield device does not parse the entire IPv6 header chain present in the packet. An implementation that has such an implementation-specific limit MUST NOT claim compliance with this specification, and MUST pass the packet when such implementation-specific limit is reached.

2. When parsing the IPv6 header chain, if the packet is a first-fragment (i.e., a packet containing a Fragment Header with the Fragment Offset set to 0) and it fails to contain the entire IPv6 header chain (i.e., all the headers starting from the IPv6 header up to, and including, the upper-layer header), DHCPv6-Shield MUST drop the packet, and SHOULD log the packet drop event in an implementation-specific manner as a security fault.

   RATIONALE: [I-D.ietf-6man-oversized-header-chain] specifies that the first-fragment (i.e., the fragment with the Fragment Offset set to 0) MUST contain the entire IPv6 header chain, and allows intermediate systems such as routers to drop those packets that fail to comply with this requirement.

   NOTE: This rule should only be applied to IPv6 fragments with a Fragment Offset of 0 (non-first fragments can be safely passed, since they will never reassemble into a complete datagram if they are part of a DHCPv6 packet meant for a DHCPv6 client received on a port where such packets are not allowed).

3. When parsing the IPv6 header chain, if the packet is identified to be a DHCPv6 packet meant for a DHCPv6 client, DHCPv6-Shield MUST drop the packet, and SHOULD log the packet drop event in an implementation-specific manner as a security fault.

4. In all other cases, DHCPv6-Shield MUST pass the packet as usual.

NOTE: For the purpose of enforcing the DHCPv6-Shield filtering policy, an ESP header [RFC4303] should be considered to be an "upper-layer protocol" (that is, it should be considered the last header in the IPv6 header chain). This means that packets employing ESP would be passed by the DHCPv6-Shield device to the intended destination. If the destination host does not have a security association with the sender of the aforementioned IPv6 packet, the packet would be dropped. Otherwise, if the packet is considered valid by the IPsec implementation at the receiving host and encapsulates a DHCPv6 message, it is up to the receiving host what to do with such packet.

If a packet is dropped due to this filtering policy, then the packet drop event SHOULD be logged in an implementation-specific manner as a security fault. The logging mechanism SHOULD include a drop counter dedicated to DHCPv6-Shield packet drops.

In order to protect current end-node IPv6 implementations, Rule #2 has been defined as a default rule to drop packets that cannot be positively identified as not being DHCPv6 packets meant for DHCPv6 clients (because the packet is a fragment that fails to include the entire IPv6 header chain). This means that, at least in theory, DHCPv6-Shield could result in false-positive blocking of some legitimate (non DHCPv6-server) packets. However, as noted in [I-D.ietf-6man-oversized-header-chain], IPv6 packets that fail to include the entire IPv6 header chain are virtually impossible to police with state-less filters and firewalls, and hence are unlikely to survive in real networks. [I-D.ietf-6man-oversized-header-chain] requires that hosts employing fragmentation include the entire IPv6 header chain in the first fragment (the fragment with the Fragment Offset set to 0), thus eliminating the aforementioned false positives.

The aforementioned filtering rules implicitly handle the case of fragmented packets: if the DHCPv6-Shield device fails to identify the upper-layer protocol as a result of the use of fragmentation, the corresponding packets would be dropped.

Finally, we note that IPv6 implementations that allow overlapping fragments (i.e. that do not comply with [RFC5722]) might still be subject of DHCPv6-based attacks. However, a recent assessment of

IPv6 implementations [SI6-FRAG] with respect to their fragment reassembly policy seems to indicate that most current implementations comply with [RFC5722].

4. IANA Considerations

This document has no actions for IANA.

5. Security Considerations

The mechanism specified in this document can be used to mitigate DHCPv6-based attacks. Attack vectors based on other messages (such as ICMPv6 Router Advertisements) are out of the scope of this document.

As noted in Section 3, IPv6 implementations that allow overlapping fragments (i.e. that do not comply with [RFC5722]) might still be subject of DHCPv6-based attacks. However, most current implementations seem to comply with [RFC5722], and hence forbid IPv6 overlapping fragments.

We note that if an attacker sends a fragmented DHCPv6 packets on a port not allowed to send such packets, the first-fragment would be dropped, and the rest of the fragments would be passed. This means that the victim node would tie memory buffers for the aforementioned fragments, which would never reassemble into a complete datagram. If a large number of such packets were sent by an attacker, and the victim node failed to implement proper resource management for the fragment reassembly buffer, this could lead to a Denial of Service (DoS). However, this does not really introduce a new attack vector, since an attacker could always perform the same attack by sending forged fragmented datagram in which at least one of the fragments is missing. [CPNI-IPv6] discusses some resource management strategies that could be implemented for the fragment reassembly buffer.

6. Acknowledgements

The authors would like to thank (in alphabetical order) Jean-Michel Combes, Juergen Schoenwaelder, and Mark Smith, for providing valuable comments on earlier versions of this document.

This document is heavily based on the document [I-D.ietf-v6ops-ra-guard-implementation] authored by Fernando Gont. Thus, the authors would like to thank Ran Atkinson, Karl Auer, Robert Downie, Washam Fan, David Farmer, Marc Heuse, Nick Hilliard, Ray Hunter, Joel Jaeggli, Simon Perreault, Arturo Servin, Gunter van de Velde, James Woodyatt, and Bjoern A. Zeeb, for providing valuable comments on [I-D.ietf-v6ops-ra-guard-implementation], on which this document is based.

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.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5722] Krishnan, S., "Handling of Overlapping IPv6 Fragments", RFC 5722, December 2009.

[RFC6564] Krishnan, S., Woodyatt, J., Kline, E., Hoagland, J., and M. Bhatia, "A Uniform Format for IPv6 Extension Headers", RFC 6564, April 2012.

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.

[I-D.ietf-6man-oversized-header-chain]
Gont, F. and V. Manral, "Security and Interoperability

Implications of Oversized IPv6 Header Chains",
draft-ietf-6man-oversized-header-chain-02 (work in
progress), November 2012.

[I-D.ietf-v6ops-ra-guard-implementation]
Gont, F., "Implementation Advice for IPv6 Router
Advertisement Guard (RA-Guard)",
draft-ietf-v6ops-ra-guard-implementation-07 (work in
progress), November 2012.

[SI6-FRAG]
SI6 Networks, "IPv6 NIDS evasion and improvements in IPv6
fragmentation/reassembly", 2012, <http://
blog.si6networks.com/2012/02/
ipv6-nids-evasion-and-improvements-in.html>.

[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

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

Email: liushucheng@huawei.com

Gunter Van de Velde
Cisco Systems
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 2704 5473
Email: gunter@cisco.com