Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 7610
BCP 199
Catégorie : Bonnes pratiques actuelles
ISSN : 2070-1721

F. Gont, SI6 Networks / UTN-FRH
W. Liu, Huawei Technologies
G. Van de Velde, Alcatel-Lucent
août 2015
Traduction Claude Brière de L'Isle

Bouclier DHCPv6 : protection contre les serveurs DHCPv6 félons

Résumé
Le présent document spécifie un mécanisme pour protéger les hôtes connectés à un réseau commuté contre des serveurs DHCPv6 félons. Il se fonde sur le filtrage de paquet DHCPv6 à l'appareil de couche 2 auquel les paquets sont reçus. Un mécanisme similaire a été largement déployé dans les réseaux IPv4 ('usurpation DHCP') ; donc, il est souhaitable qu'une fonctionnalité similaire soit fournie pour les réseaux IPv6. Le présent document spécifie les bonnes pratiques actuelles pour la mise en œuvre d'un bouclier DHCPv6.

Table des Matières

1. Introduction

Le présent document spécifie le bouclier DHCPv6, un mécanisme pour protéger les hôtes connectés à un réseau commuté contre les serveurs DHCPv6 félons [RFC3315]. Le concept de base derrière le bouclier DHCPv6 est qu'un appareil de couche 2 filtre les messages DHCPv6 destinés aux clients DHCPv6 (qu'on appellera désormais, "messages de serveur DHCPv6") selon un certain nombre de critères différents. Le critère de filtrage le plus basique est que les messages de serveur DHCPv6 soient éliminés par l'appareil de couche 2 sauf si ils sont reçus sur des accès spécifiques de l'appareil de couche 2.

Avant que l'appareil de bouclier DHCPv6 soit déployé, l'administrateur spécifie le ou les accès de couche 2 sur lesquels les messages de serveur DHCPv6 sont permis. Seuls ces accès auxquels un serveur ou relais DHCPv6 doit se connecter devraient être spécifiés comme tels. Une fois déployé, l'appareil de bouclier DHCPv6 inspecte les paquets reçus et ne permet (c'est-à-dire, ne passe) les messages de serveur DHCPv6 que si ils sont reçus sur un accès de couche 2 qui a été explicitement configuré à cette fin.

Le bouclier DHCPv6 est analogue au mécanisme de garde d'annonce de routeur (RA-Guard, *Router Advertisement Guard*) [RFC6104], [RFC6105], [RFC7113], destiné à la protection contre les messages d'annonce de routeur félons [RFC4861].

On note que le bouclier DHCPv6 atténue seulement les attaques fondées sur DHCPv6 contre les hôtes. Les vecteurs d'attaque fondés sur d'autres messages destinés à la configuration du réseau (comme les annonces de routeur ICMPv6) ne sont pas visés par le bouclier DHCPv6 lui-même. Dans une veine similaire, le bouclier DHCPv6 n'atténue pas les attaques contre les serveurs DHCPv6 (par exemple, de déni de service).

2. Langage des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Terminologie

Bouclier DHCPv6 : ensemble de règles de filtrage spécifié dans le présent document, destiné à atténuer les attaques qui emploient des paquets de serveur DHCPv6.

Appareil de bouclier DHCPv6 : appareil de couche 2 (normalement un commutateur de couche 2) qui met en application la politique de filtrage spécifiée dans le présent document.

Pour les besoins du présent document, les termes "en-tête d'extension IPv6", "premier fragment", "chaîne d'en-tête IPv6", et "en-tête de couche supérieure" sont utilisés comme spécifié dans la [RFC7112]:

En-tête d'extension IPv6r : les en-têtes d'extension IPv6 sont définis à la Section 4 de la [RFC2460]. Par suite de la [RFC7045], [IANA-PROTO] donne la liste des numéros alloués du protocole Internet et désigne quels numéros de protocole représentent aussi des en-têtes d'extension IPv6.

Premier fragment : fragment IPv6 avec un décalage de fragment égal à 0.

Chaîne d'en-tête IPv6 : la chaîne d'en-tête IPv6 contient un en-tête IPv6 initial, zéro, un ou plusieurs en-têtes d'extension IPv6, et facultativement, un seul en-tête de couche supérieure. Si un en-tête de couche supérieure est présent, il termine la chaîne d'en-têtes IPv6 ; autrement, la valeur "Pas de prochain en-tête" (Prochain en-tête = 59) la termine.Le premier membre de la chaîne d'en-tête IPv6 est toujours un en-tête IPv6. Pour qu'un en-tête suivant se qualifie comme membre de la chaîne d'en-têtes IPv6, il doit être référencé par le champ "Prochain en-tête" du membre précédent de la chaîne d'en-têtes IPv6. Cependant, si un second en-tête IPv6 apparaît dans la chaîne d'en-têtes IPv6, comme c'est le cas quand IPv6 est tunnelé sur IPv6, le second en-tête IPv6 est considéré comme un en-tête de couche supérieure et termine la chaîne d'en-têtes IPv6. De même, si un en-tête d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) apparaît dans la chaîne d'en-têtes IPv6, il est considéré comme un en-tête de couche supérieure, et il termine la chaîne d'en-têtes IPv6.

En-tête de couche supérieure : en général, l'en-tête de couche supérieure est le premier membre de la chaîne d'en-têtes qui n'est ni un en-tête IPv6 ni un en-tête d'extension IPv6. Cependant, si un en-tête ESP ou un second en-tête IPv6 se produit dans la chaîne d'en-têtes IPv6, il est considéré comme étant un en-tête de couche supérieure, et il termine la chaîne d'en-têtes IPv6.

Ni la charge utile de couche supérieure ni aucune données de protocole suivant la charge utiles de couche supérieure ne sont considérées faire partie de la chaîne d'en-têtes IPv6. Dans un exemple simple, si l'en-tête de couche supérieure est un en-tête TCP, la charge utile TCP ne fait pas partie de la chaîne d'en-têtes IPv6. Dans un exemple plus complexe, si l'en-tête de couche supérieure est un en-tête ESP, ni les données de la charge utile, ni aucun des champs qui suivent les données de la charge utile dans l'en-tête ESP ne font partie de la chaîne d'en-têtes IPv6.

4. Configuration du bouclier DHCPv6

Avant d'être déployé pour production, l'appareil de bouclier DHCPv6 est explicitement configuré par rapport aux accès de couche 2 qui sont permis pour recevoir des paquets DHCPv6 destinés aux clients DHCPv6 (c'est-à-dire, les messages de serveur DHCPv6). Seuls les accès de couche 2 explicitement configurés à cette fin peuvent recevoir des paquets DHCPv6 à passer aux clients DHCPv6.

5. Exigences pour la mise en œuvre du bouclier DHCPv6

Voici les règles de filtrage qui sont mises en application au titre d'une mise en œuvre de bouclier DHCPv6 sur les accès auxquels il n'est pas permis de recevoir des paquets DHCPv6 pour les clients DHCPv6 :

1. Les mises en œuvre de bouclier DHCPv6 DOIVENT analyser la chaîne d'en-têtes IPv6 entière présente dans le paquet à identifier comme étant ou non un paquet DHCPv6 destiné au client DHCPv6 (c'est-à-dire, un message de serveur DHCPv6).

RAISON : Les mises en œuvre de bouclier DHCPv6 NE DOIVENT PAS appliquer de limite au nombre d'octets qu'elles peuvent inspecter (en commençant par le début du paquet IPv6) car cela pourrait introduire des faux négatifs: Les paquets de serveur DHCP6 reçus sur des accès auxquels il n'est pas permis de recevoir de tels paquets pourraient être permis simplement parce que l'appareil de bouclier DHCPv6 n'analyse pas la chaîne entière d'en-têtes IPv6 présents dans le paquet

2. Lors de l'analyse de la chaîne d'en-têtes IPv6, si le paquet est un premier fragment (c'est-à-dire, un paquet contenant un en-tête Fragment avec le décalage de fragment réglé à 0) et si il manque à contenir la chaîne entière d'en-têtes IPv6 (c'est-à-dire, tous les en-têtes en commençant par l'en-tête IPv6 jusqu'à, et y compris, l'en-tête de couche supérieure) le bouclier DHCPv6 DOIT éliminer le paquet et devrait enregistrer l'événement d'élimination de paquet d'une manière spécifique de la mise en œuvre comme faute de sécurité.

RAISON : Les paquets qui ne contiennent pas la chaîne entière d'en-têtes IPv6 pourraient autrement être utilisés pour circonvenir le bouclier DHCPv6. La [RFC7112] exige que le premier fragment (c'est-à-dire, le fragment avec le décalage de fragment réglé à 0) contienne la chaîne d'en-têtes IPv6 entière. La [RFC7112] permet aussi que les systèmes intermédiaires comme les routeurs éliminent les paquets qui ne satisfont pas cette exigence.

Note : Cette règle ne devrait s'appliquer qu'aux fragments IPv6 avec un décalage de fragment de 0 (les fragments non premiers peuvent être passés en toute sécurité, car ils ne vont jamais se rassembler en un datagramme complet si ils font partie d'un paquet DHCPv6 destiné à un client DHCPv6 reçu sur un accès où de tels paquets ne sont pas permis).

3. Le bouclier DHCPv6 DOIT fournir un bouton de configuration qui contrôle si les paquets d'une valeur de "Prochain en-tête" non reconnue sont éliminés ou non ; ce bouton de configuration DOIT être par défaut "éliminer". Lors de l'analyse de la chaîne d'en-têtes IPv6, si le paquet contient une valeur de "Prochain en-tête" non reconnue et si le bouton de configuration est configuré à "éliminer", le bouclier DHCPv6 DOIT éliminer le paquet et devrait enregistrer l'événement d'élimination du paquet d'une manière spécifique de la mise en œuvre comme faute de sécurité.

RAISON : Une valeur de "Prochain en-tête" non reconnue pourrait éventuellement identifier un en-tête d'extension IPv6 et donc être utilisée pour dissimuler un paquet de serveur DHCPv6 (comme il n'y a aucun moyen pour un bouclier DHCPv6 d'analyser des valeurs de Prochain en-tête passées non reconnues [IPV6-UEH]). La [RFC7045] exige que les nœuds soient configurables quant à la question de savoir si les paquets avec des en-têtes non reconnus sont transmis ou non, et de permettre que le comportement par défaut soit que de tels paquets soient éliminés.

4. Lors de l'analyse de la chaîne d'en-têtes IPv6, si le paquet est identifié comme paquet DHCPv6 destiné à un client DHCPv6, le bouclier DHCPv6 DOIT éliminer le paquet et DEVRAIT enregistrer l'événement d'élimination de paquet d'une manière spécifique de la mise en œuvre comme alerte de sécurité.

RAISON : En fin de compte, le but du bouclier DHCPv6 est d'éliminer les paquets DHCPv6 destinés aux clients DHCPv6 (c'est-à-dire, les messages de serveur DHCPv6) qui sont reçus sur des accès qui n'ont pas été explicitement configurés à permettre la réception de tels paquets.

5. Dans tous les autres cas, le bouclier DHCPv6 DOIT passer le paquet comme d'habitude.

Note : Pour les besoins de l'application de la politique de filtrage du bouclier DHCPv6, un en-tête ESP [RFC4303] devrait être

considéré comme de "protocole de couche supérieure" (c'est-à-dire, il devrait être considéré comme le dernier en-tête dans la chaîne d'en-têtes IPv6). Cela signifie que les paquets qui emploient ESP seraient passés par l'appareil de bouclier DHCPv6 à la destination prévue. Si l'hôte de destination n'a pas d'association de sécurité avec l'envoyeur du paquet IPv6 susmentionné, le paquet sera éliminé. Autrement, si le paquet est considéré comme valide par la mise en œuvre IPsec chez l'hôte receveur et encapsule un message DHCPv6, ce qu'il convient de faire d'un tel paquet regarde l'hôte receveur.

Les règles ci-dessus indiquent que si un paquet est éliminé à cause de cette politique de filtrage, l'événement d'élimination du paquet devrait être enregistré d'une manière spécifique de la mise en œuvre comme faute de sécurité. Il est utile pour le mécanisme d'enregistrement d'inclure un compteur d'éliminations par accès dédié aux éliminations de paquets DHCPv6 du bouclier.

Afin de protéger les mises en œuvre actuelles de nœud d'extrémité IPv6, la règle n° 2 a été définie de façon à ce que le comportement par défaut soit que les paquets qui ne peuvent pas être positivement identifiés comme n'étant pas des paquets de serveur DHCPv6 (parce que le paquet est un fragment qui échoue à inclure la chaîne entière d'en-têtes IPv6) soient éliminés. Cela signifie que, au moins en théorie, le bouclier DHCPv6 pourrait résulter en des faux positifs bloquant certains paquets légitimes (qui ne sont pas de serveur DHCPv6). Cependant, comme le note la [RFC7112], les paquets IPv6 qui échouent à inclure la chaîne d'en-têtes IPv6 entière sont virtuellement impossibles à réguler avec des filtres sans état et des pare-feu ; donc, il est peu probable qu'ils survivent dans les vrais réseaux. La [RFC7112] exige que les hôtes qui emploient la fragmentation incluent la chaîne d'en-têtes IPv6 entière dans le premier fragment (le fragment qui a le décalage de fragment réglé à 0) éliminant donc les faux positifs susmentionnés.

Les règles de filtrage ci-dessus traitent implicitement le cas des paquets fragmentés : si l'appareil de bouclier DHCPv6 échoue à identifier le protocole de couche supérieure par suite de l'utilisation de la fragmentation, les paquets correspondants seraient éliminés.

Finalement, on note que les mises en œuvre de IPv6 qui permettent le chevauchement de fragments (c'est-à-dire, qui ne se conforment pas à la [RFC5722]) peuvent encore être l'objets d'attaques fondées sur DHCPv6. Cependant, une évaluation récente des mises en œuvre IPv6 [SI6-FRAG] par rapport à leur politique de réassemblage de fragments semble indiquer que la plupart d'entre elles se conforment à la [RFC5722].

6. Considérations sur la sécurité

Les recommandations du présent document représentent le comportement idéal d'un appareil de bouclier DHCPv6. Cependant, afin de mettre en œuvre rapidement un bouclier DHCPv6, il peut être nécessaire de limiter la profondeur à laquelle le paquet peut être examiné avant d'abandonner. Dans des circonstances où il y a une telle limitation, il est recommandé que les mises en œuvre éliminent les paquets après avoir tenté de trouver un en-tête de protocole jusqu'à cette limite, quelle qu'elle soit. Idéalement, de tels appareils devraient être configurables avec une liste d'identifiants d'en-tête de protocole, afin que si de nouveaux protocoles de transport sont normalisés après la livraison de l'appareil, ils puissent être ajoutés à la liste des types d'en-tête de protocole que reconnaît l'appareil. Comme tout en-tête de protocole qui n'est pas un en-tête UDP va être passé par l'algorithme de bouclier DHCPv6, cela va permettre à ces appareils d'éviter de bloquer l'utilisation de nouveaux protocoles de transport. Lorsque une mise en œuvre doit arrêter ses recherches de types d'en-têtes reconnaissables dans un paquet à cause de telles limitations, l'appareil DEVRAIT être configurable soit à passer, soit à éliminer le paquet.

Le mécanisme spécifié dans ce document peut être utilisé pour atténuer les attaques fondées sur DHCPv6 contre les hôtes. Les vecteurs d'attaque fondée sur d'autres messages destinés à la configuration de réseau (comme les annonces de routeur ICMPv6) sortent du domaine d'application du présent document. De plus, le mécanisme spécifié dans ce document n'a pas d'effet sur les attaques contre les serveurs DHCPv6 (par exemple, de déni de service).

Si il est déployé dans un domaine de couche 2 avec plusieurs commutateurs en cascade, il y aura un accès d'entrée sur le commutateur local de l'hôte qui aura besoin d'être en capacité de recevoir des messages de serveur DHCPv6. Cependant, ce commutateur local va dépendre du filtrage des messages de serveur DHCPv6 félons par les appareils en amont, car le commutateur local n'a aucun moyen de déterminer quels messages de serveur DHCP amont sont valides. Donc, afin d'être efficace, le bouclier DHCPv6 devrait être déployé et activé sur tous les commutateurs de couche 2 d'un domaine de couche 2.

Comme noté à la Section 5, les mises en œuvre de IPv6 qui permettent le chevauchement de fragments (c'est-à-dire, qui ne se conforment pas à la [RFC5722]) peuvent encore être l'objet d'attaques fondées sur DHCPv6. Cependant, la plupart des mises en œuvre courantes semblent se conformer à la [RFC5722] et donc interdire le chevauchement de fragments IPv6.

On note que si un attaquant envoie un paquet DHCPv6 fragmenté sur un accès auquel il n'est pas permis de recevoir de tels paquets, le premier fragment sera éliminé, et le reste des fragments sera passé. Cela signifie que le nœud victime va remplir ses mémoires tampon de ces fragments, qui ne vont jamais se rassembler en datagrammes complets. Si un grand nombre de ces

paquets était envoyé par un attaquant, et si le nœud victime échouait à mettre en œuvre la gestion des ressources appropriée pour la mémoire tampon de rassemblement de fragments, cela pourrait conduire à un déni de service. Cependant, cela n'introduit pas réellement un nouveau vecteur d'attaque, car un attaquant pourrait toujours effectuer la même attaque en envoyant des fragments de datagramme falsifiés dans lesquels au moins un des fragments manquerait. [CPNI-IPv6] discute des stratégies de gestion de ressource qui pourraient être mises en œuvre pour la mémoire tampon de rassemblement de fragments.

On note de plus que la sécurité d'un site qui emploie un bouclier DHCPv6 pourrait être encore améliorée en déployant la [RFC7513] pour atténuer les attaques d'adresse IPv6 falsifiée.

Finalement, on note que d'autres mécanismes pour atténuer les attaques fondées sur les messages de serveur DHCPv6 sont disponibles et qui ont des considérations de déploiement différentes. Par exemple, [SECURE-DHCPV6] permet l'authentification des paquets de serveur DHCPv6 si les adresses IPv6 des serveurs DHCPv6 peuvent être préconfigurées sur les nœuds clients.

4. Références

4.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997, DOI 10.17487/RFC2119.

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1998. *(MàJ par* 5095, 6564 *; D.S ; Remplacée par* RFC8200, STD 86*)*, DOI 10.17487/RFC2460.

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. DOI 10.17487/RFC3315 (*Rendue obsolète par* RFC8415)

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*, DOI 10.17487/RFC4303.

[RFC4861] T. Narten et autres, "Découverte du voisin pour IP version 6 (IPv6)", septembre 2007. (*Remplace* RFC2461 ; *D.S. ; MàJ par* RFC8028, RFC8319, RFC8425), DOI 10.17487/RFC4861.

[RFC5722] S. Krishnan, "Traitement des fragments IPv6 en chevauchement", décembre 2009. *(P. S.)*, DOI 10.17487/RFC5722.

[RFC7045] B. Carpenter, S. Jiang, "Transmission et traitement des en-têtes d'extension IPv6", décembre 2013. (*MàJ* RFC2460, RFC2780) *(P.S.)*, DOI 10.17487/RFC7045.

[RFC7112] F. Gont, V. Manral, R. Bonica, "Implications des chaînes d'en-tête IPv6 surdimensionnées", janvier 2014. (*MàJ* RFC2460) *(P.S.)*, DOI 10.17487/RFC7112.

7.2 Références pour information

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

[IANA-PROTO] IANA, "Protocol Numbers", < http://www.iana.org/assignments/protocol-numbers >.

[IPV6-UEH] Gont, F., Liu, W., Krishnan, S., and H. Pfeifer, "IPv6 Universal Extension Header", Travail en cours, draft-gont-6man-rfc6564bis-00, avril 2014.

[RFC6104] T. Chown, S. Venaas. "Position du problème des fausses annonces de routeur IPv6", février 2011. *(Information)*, DOI 10.17487/RFC6104.

[RFC6105] E. Levy-Abegnoli et autres, "Protection des annonces de routeur IPv6 ", février 2011. *(Info.)*, DOI 10.17487/RFC6105.

[RFC7113] F. Gont, "Conseil de mise en œuvre pour la garde d'annonce de routeur IPv6 (RA-Guard)", février 2014. (*MàJ*

RFC6105) *(Information)*, DOI 10.17487/RFC7113.

[RFC7513] J. Bi, J. Wu, G. Yao, F. Baker, "Solutions d'amélioration de la validation de l'adresse de source (SAVI) pour DHCP", mai 2015. *(P.S.)*, DOI 10.17487/RFC7513.

[SECURE-DHCPV6] Jiang, S. and S. Shen, "Secure DHCPv6 Using CGAs", Travail en cours, draft-ietf-dhc-secure-dhcpv6-07, septembre 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 >.

Remerciements

Les auteurs tiennent à remercier Mike Heard, qui a fourni des retours détaillés sur les versions antérieures de ce document et a beaucoup aidé à produire un document techniquement valide à travers tout le processus de publication.

Les auteurs tiennent aussi à remercier (par ordre alphabétique) Ben Campbell, Jean-Michel Combes, Sheng Jiang, Ted Lemon, Pete Resnick, Carsten Schmoll, Juergen Schoenwaelder, Robert Sleigh, Donald Smith, Mark Smith, Hannes Tschofenig, Eric Vyncke, et Qin Wu pour leurs précieux commentaires sur les versions antérieures ce ce document.

Une partie de la Section 3 du document est empruntée à la [RFC7112], dont les auteurs sont Fernando Gont, Vishwas Manral, et Ron Bonica.

Le présent document est largement fondé sur la [RFC7113], dont l'auteur est Fernando Gont. Donc, les auteurs tiennent à remercier les individus suivants qui ont fourni des commentaires précieux sur la [RFC7113] : Ran Atkinson, Karl Auer, Robert Downie, Washam Fan, David Farmer, Mike Heard, Marc Heuse, Nick Hilliard, Ray Hunter, Joel Jaeggli, Simon Perreault, Arturo Servin, Gunter Van de Velde, James Woodyatt, et Bjoern A. Zeeb.

Les auteurs remercient Joel Jaeggli de ses avis et conseils tout au long du processus de l'IETF.

Fernando Gont aimerait remercier Diego Armando Maradona de sa magie et son inspiration.

Adresse des auteurs

Fernando Gont
SI6 Networks / UTN-FRH
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina
mél : fgont@si6networks.com
URI : http://www.si6networks.com

Will (Shucheng) Liu
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
China
mél : liushucheng@huawei.com

Gunter Van de Velde
Alcatel-Lucent
Copernicuslaan 50
Antwerp, Antwerp 2018
Belgium
mél : gunter.van_de_velde@alcatel-lucent.com