

Groupe de travail Réseau
Request for Comments : 3646
 Catégorie : En cours de normalisation

R. Droms, éditeur, Cisco Systems
 décembre 2003
 Traduction Claude Brière de L'Isle

Options de configuration du DNS pour le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)

Statut de ce mémoire

Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2003). Tous droits réservés.

Résumé

Le présent document décrit les options du protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6, *Dynamic Host Configuration Protocol for IPv6*) pour passer une liste des serveurs de noms DNS récurrents disponibles et une liste de recherche de domaines à un client.

1. Introduction

Le présent document décrit deux options pour passer les informations de configuration qui se rapportent au service des noms de domaines (DNS, *Domain Name Service*) ([RFC1034] et [RFC1035]) dans DHCPv6 ([RFC3315]).

2. Terminologie

Les mots-clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" lorsque ils apparaissent dans le présent document sont à interpréter comme décrit dans le BCP 14, [RFC 2119].

Tout au long du présent document, sauf spécification contraire, l'acronyme DHCP se réfère à DHCP pour IPv6 (DHCPv6) comme spécifié dans la [RFC3315].

Le présent document utilise la terminologie spécifique d'IPv6 et de DHCP comme défini à la section 4 "Terminologie" de la [RFC3315].

3. Option Serveur de noms DNS récurrent

L'option Serveur de noms DNS récurrent fournit une liste d'une ou plusieurs adresses IPv6 de serveurs de noms DNS récurrents auxquels le résolveur DNS d'un client PEUT envoyer des interrogations DNS [RFC1035]. Les serveurs DNS sont énumérés dans l'ordre de préférence de l'utilisation par le résolveur du client.

Le format de l'option Serveur de noms DNS récurrent est :

```

      0                               1                               2                               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|          OPTION_DNS_SERVEUR          |   Longueur d'option   |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |                           |
|          Serveur-de-noms-DNS-récurrent (adresse IPv6)         |
|                                     |                           |
|                                     |                           |
+-----+-----+-----+-----+-----+-----+-----+-----+

```


Le degré de vulnérabilité d'un hôte aux attaques via une option invalide de recherche de domaine est déterminé en partie par le comportement du résolveur DNS. La [RFC1535] contient un exposé des faiblesses de la sécurité à l'égard des listes de recherche de domaine implicites aussi bien qu'explicites, et formule des recommandations sur le traitement des listes de recherche par les résolveurs. La Section 6 de la [RFC1536] traite aussi de cette vulnérabilité, et recommande que les résolveurs :

1. N'utilisent des listes de recherche que lorsque explicitement spécifié ; aucune liste de recherche implicite ne devrait être utilisée.
2. Résolvent un nom qui contient des points en l'essayant d'abord comme FQDN et si cela échoue, avec les noms dans la liste de recherche associée.
3. Résolvent un nom ne contenant pas de point en l'ajoutant directement à la liste de recherche, mais là encore, aucune liste de recherche implicite ne devrait être utilisée.

Afin de minimiser les faiblesses potentielles, il est recommandé que :

1. Les hôtes qui mettent en œuvre l'option de recherche de domaine DEVRAIENT aussi mettre en œuvre les recommandations sur la liste de recherche de la section 6 de la RFC1536.
2. Lorsque des paramètres DNS tels que la liste de recherche de domaines ou des serveurs DNS ont été configurés manuellement, ces paramètres NE DEVRAIENT PAS être outrepassés par DHCP.
3. Un hôte DEVRAIT exiger l'utilisation de l'authentification DHCP (Voir à la section 21 "Authentification des messages DHCP" de la RFC3315) avant d'accepter une option de recherche de domaine.

7. Considérations relatives à l'IANA

L'IANA a alloué un code d'option à l'option Serveur de noms DNS récurrent (23) et à l'option Liste de domaine de recherche (24) à partir de l'espace de code d'option DHCP défini à la section "Considérations relatives à l'IANA" de la [RFC3315].

8. Remerciements

Cette option faisait à l'origine partie de la spécification DHCPv6, écrite par Jim Bound, Mike Carney, Charlie Perkins, Ted Lemon, Bernie Volz et Ralph Droms.

L'analyse de l'attaque potentielle à travers la liste de recherche de domaine est tirée de la spécification de l'option Recherche de domaine de DHCPv4, [RFC3397].

Merci à Rob Austein, Alain Durand, Peter Koch, Tony Lindstrom et Pekka Savola pour leurs contributions au présent document.

9. Références

9.1 Références normatives

[RFC1035] P. Mockapetris, "Noms de domaines – [Mise en œuvre](#) et spécification", STD 13, novembre 1987.

[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.

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

[RFC2535] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir RFC4033, RFC4034, RFC4035*) (P.S.)

[RFC1536] A. Kumar, J. Postel, C. Neuman, P. Danzig, S. Miller, "Erreurs courantes de mise en œuvre du DNS et corrections suggérées", octobre 1993. (*Information*)

9.2 Références pour information

[RFC1034] P. Mockapetris, "Noms de domaines - [Concepts et facilités](#)", STD 13, novembre 1987.

- [RFC1535] E. Gavron, "Problème de sécurité et proposition de correction avec le logiciel courant du DNS", octobre 1993. (*Information*)
- [RFC3397] B. Aboba, S. Cheshire, "Option Recherche de domaine du protocole de configuration dynamique d'hôte (DHCP)", novembre 2002. (*P.S.*)

Déclaration de droits de propriété intellectuelle

L'IETF ne prend position sur la validité ou la portée d'aucun droit de propriété intellectuelle ou d'autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou non disponible ; pas plus qu'elle ne prétend qu'elle ait fait aucun effort pour identifier de tels droits. Des informations sur les procédures de l'IETF au sujet des droits dans la documentation en cours de normalisation et en rapport avec les normes peuvent être trouvées dans le BCP-11. Des copies des revendications de droits peuvent être disponibles à la publication et toutes les assurances de licences peuvent être rendues disponibles, ou le résultat de tentatives d'obtention d'une licence ou permission générale pour l'utilisation de tels droits de propriété par les mises en œuvre ou utilisateurs de la présente spécification peuvent être obtenus auprès du secrétariat de l'IETF.

L'IETF invite toute partie intéressée à porter à son attention tous droits de reproduction, brevets ou applications de brevets, ou autres droits de propriété qui pourraient couvrir une technologie qui pourrait être nécessaire pour mettre en pratique la présente norme. Prière d'adresser les informations au Directeur Général de l'IETF.

Adresse de l'auteur

Ralph Droms, Editor
Cisco Systems
1414 Massachusetts Ave.
Boxboro, MA 01719
USA
téléphone : +1 978 936 1674
mél : rdroms@cisco.com

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2003). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de copyright ci-dessus et le présent et paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de copyright ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de copyright définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou successeurs ou ayant droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.