Groupe de travail Réseau
Request for Comments : 5095
RFC mises à jour : 2460, 4294
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Abley, Afilias
P. Savola, CSC/FUNET
G. Neville-Neil, Neville-Neil Consulting
décembre 2007

Les en-têtes d'acheminement de type 0 sont déconseillés dans IPv6

Résumé
La fonctionnalité fournie par l'en-tête d'acheminement IPv6 de type 0 peut être exploitée afin de réaliser une amplification de trafic sur un chemin distant dans le but de générer une attaque de déni de service. Le présent document met à jour la spécification IPv6 pour déconseiller l'utilisation des en-têtes d'acheminement IPv6 de type 0, à la lumière de ce problème de sécurité.

Table des Matières

1. Introduction

La [RFC2460] définit un en-tête d'extension IPv6 appelé "en-tête d'acheminement", identifié par une valeur de Prochain en-tête de 43 dans l'en-tête immédiatement précédent. Un sous-type particulier d'en-tête d'acheminement noté comme "type 0" est aussi défini. Les en-têtes d'acheminement de type 0 sont appelés "RH0" dans ce document.

Un seul RH0 peut contenir plusieurs adresses de nœuds intermédiaires, et la même adresse peut être incluse plus d'une fois dans le même RH0. Cela permet qu'un paquet soit construit de telle façon qu'il oscille de nombreuses fois entre deux hôtes ou routeurs qui traitent le RH0. Cela permet qu'un flux de paquets provenant d'un attaquant soit amplifié le long du chemin entre deux routeurs distants, ce qui pourrait être utilisé pour causer de l'encombrement le long de chemins distants arbitraires et donc agir comme un mécanisme de déni de service. Une amplification de 88 fois a été montrée en utilisant cette technique [CanSecWest07].

Cette attaque est particulièrement sérieuse en ce qu'elle affecte le chemin entier entre les deux nœuds exploités, et non seulement les nœuds eux-mêmes ou leurs réseaux locaux. Une fonctionnalité analogue se trouve dans l'option Route de source de IPv4, mais les opportunités d'abus sont plus grandes avec RH0 du fait de la capacité de spécifier beaucoup plus d'adresses de nœuds intermédiaires dans chaque paquet.

La sévérité de cette menace est considérée comme suffisante pour justifier de déconseiller entièrement RH0. Un effet collatéral est que cela élimine aussi les cas d'utilisation bénine de RH0 ; cependant, de telles applications pourront être facilitées par de futures spécifications d'en-tête d'acheminement.

Les problèmes potentiels de RH0 ont été identifiés en 2001 [Security]. En 2002 une proposition a été faite de restreindre le traitement de l'en-tête d'acheminement dans les hôtes [Hosts]. Ces efforts ont résulté en la modification de la spécification IPv6 mobile pour utiliser l'en-tête d'acheminement de type 2 au lieu de celui de la [RFC3775]. Vishwas Manral a identifié divers risques associés à RH0 en 2006 incluant l'attaque d'amplification ; plusieurs de ces vulnérabilités (avec d'autres problèmes) ont été ultérieurement documentés dans la [RFC4942].

Un traitement des implications opérationnelles de sécurité de RH0 a été présenté par Philippe Biondi et Arnaud Ebalard à la conférence CanSecWest à Vancouver, en 2007 [CanSecWest07]. Cette présentation a résulté en une large publicité sur les risques associés à RH0.

Le présent document met à jour les [RFC2460] et [RFC4294].

2. Définitions

RH0 dans le présent document note l'en-tête d'extension IPv6 de type 43 ("en-tête d'acheminement") variante 0 ("en-tête d'acheminement de type 0") comme défini dans la [RFC2460].

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. RH0 est déconseillé

Un nœud IPv6 qui reçoit un paquet avec une adresse de destination qui lui est allouée et qui contient un en-tête d'extension RH0 NE DOIT PAS exécuter l'algorithme spécifié dans la dernière partie du paragraphe 4.4 de la [RFC2460] pour RH0. À la place, de tels paquets DOIVENT être traités en accord avec le comportement spécifié au paragraphe 4.4 de la [RFC2460] pour un datagramme qui inclut une valeur de type d'acheminement non reconnue, à savoir :

Si Segments restants est zéro, le nœud doit ignorer l'en-tête d'acheminement et continuer de traiter le prochain en-tête dans le paquet, dont le type est identifié par le champ Prochain en-tête dans l'en-tête d'acheminement.

Si Segments restants est différent de zéro, le nœud doit éliminer le paquet et envoyer un message ICMP Problème de paramètre, code 0, à l'adresse de source du paquet, pointant sur le type d'acheminement non reconnu.

Les mises en œuvre de IPv6 ne soit plus requises de mettre en œuvre RH0 de quelque manière que ce soit.

4. Fonctionnement

4.1 Filtrage d'entrée

On s'attend à ce qu'il faille un peu de temps avant que tous les nœuds IPv6 soient mis à jour pour supprimer la prise en charge de RH0. Certaines des utilisations de RH0 décrites dans [CanSecWest07] peuvent être atténuées en utilisant le filtrage d'entrée, comme recommandé dans les [RFC2827] et [RFC3704].

Une politique de sécurité de site destinée à protéger contre les attaques qui utilisent RH0 DEVRAIT inclure la mise en œuvre du filtrage d'entrée à la bordure du site.

4.2 Politique des pare-feu

Bloquer tous les paquets IPv6 qui portent des en-têtes d'acheminement (plutôt que de bloquer spécifiquement le type 0 et permettre les autres types) a des implications très sérieuses pour le futur développement de IPv6. Si même un faible pourcentage des pare-feu déployés bloquent d'autres types d'en-têtes d'acheminement par défaut, il sera impossible en pratique d'étendre les en-têtes d'acheminement IPv6. Par exemple, IPv6 mobile [RFC3775] s'appuie sur un en-tête d'acheminement de type 2 ; un blocage à grande échelle sans discrimination des en-têtes d'acheminement rendrait IPv6 mobile indéployable.

La politique de pare-feu destinée à protéger contre les paquets contenant RH0 NE DOIT PAS simplement filtrer tout le trafic avec un en-tête d'acheminement ; il doit être possible de désactiver la transmission du trafic de type 0 sans bloquer les autres types d'en-têtes d'acheminement. De plus, la configuration par défaut DOIT permettre la transmission du trafic qui utilise un en-tête d'acheminement autre que 0.

5. Considérations sur la sécurité

L'objet du présent document est de déconseiller une caractéristique de IPv6 qui s'est révélée avoir des implications de sécurité indésirables. Des exemples spécifiques des vulnérabilités qui sont facilitées par la disponibilité de RH0 se trouvent dans [CanSecWest07]. En particulier, RH0 fournit un mécanisme pour l'amplification du trafic qui pourrait être utilisé pour une attaque de déni de service. Une description de cette fonctionnalité se trouve à la Section 1.

6. Considérations relatives à l'IANA

Le registre IANA "Paramètres du Protocole Internet version 6 (IPv6)" devrait être mis à jour pour refléter que la variante 0 du type d'en-tête IPv6 43 ("En-tête d"acheminement") est déconseillée.

7. Remerciements

Le présent document a bénéficié des contributions de nombreux participants aux groupes de travail IPV6 et V6OPS, incluant Jari Arkko, Arnaud Ebalard, Tim Enos, Brian Haberman, Jun-ichiro itojun Hagino, Bob Hinden, Thomas Narten, Jinmei Tatuya, David Malone, Jeroen Massar, Dave Thaler, et Guillaume Valadon.

8. Références

8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[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*)*

[RFC4294] J. Loughney, éd., "Exigences pour les nœuds IPv6", avril 2006. (*MàJ par* RFC5095) *(Information)*

8.2 Références pour information

[CanSecWest07] Biondi, P. and A. Ebalard, "IPv6 Routing Header Security", CanSecWest Security Conference 2007, avril 2007. http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf

[Hosts] Savola, P., "Note about Routing Header Processing on IPv6 Hosts", Travail en cours, février 2002.

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC3704] F. Baker, P. Savola, "Filtrage d'entrée pour réseaux à rattachement multiples", mars 2004. (BCP0084) (*MàJ par* RFC8704)

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.) (Obs., voir* RFC6275)

[RFC4942] E. Davies et autres, "Considérations sur la sécurité pour la transition/co-existence avec IPv6", septembre 2007 *(Info.*

[Security] Savola, P., "Security of IPv6 Routing Header and Home Address Options", Travail en cours, mars 2002.

Adresse des auteurs

Joe Abley
Afilias Canada Corp.
Suite 204, 4141 Yonge Street
Toronto, ON M2P 2A8
Canada
téléphone : +1 416 673 4176
mél : jabley@ca.afilias.info

Pekka Savola
CSC/FUNET
Espoo,
Finland
mél : psavola@funet.fi

George Neville-Neil
Neville-Neil Consulting
2261 Market St. #239
San Francisco, CA 94114
USA
mél : gnn@neville-neil.com

Déclaration complète de droits de reproduction