RFC 7112 : Implications of Oversized IPv6 Header Chains

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 janvier 2014

Date de publication du RFC : Janvier 2014

https://www.bortzmeyer.org/7112.html

Résumer ce nouveau RFC en deux mots ? Il dit qu'il ne faut pas, lorsque des paquets IPv6 sont fragmentés, que les en-têtes d'extension se retrouvent dans des fragments différents. Tous ces en-têtes **doivent** être dans le premier fragment, pour des raisons de sécurité.

Ces en-têtes d'extension, une nouveauté d'IPv6, ont causé bien des casse-têtes aux développeurs, par exemple pour suivre la chaîne qu'ils représentent <https://www.bortzmeyer.org/analyse-pcap-ipv6.html>. Normalisés dans la section 4 du RFC 2460 [1], ils n'ont connu à leur début aucune limite : leur nombre pouvait être quelconque (contrairement à ce qui se passe pour IPv4, où la place réservée aux options a une taille maximale, de 40 octets). Rien ne s'opposait donc à ce que la chaîne de ces en-têtes, avant l'en-tête de transport, soit trop grosse pour tenir dans un seul fragment et soit donc coupée, une partie des en-têtes se retrouvant dans les fragments suivants. Je vous rassure tout de suite, de telles chaînes délirantes n'arrivent jamais en vrai mais, comme les logiciels étaient obligés de les gérer, elles auraient pu être créées et exploitées par des attaquants. Par exemple, un attaquant peut fabriquer délibérement une chaîne d'en-têtes très longue, de façon à ce que les informations de la couche transport soient dans le deuxième paquet, que certains IDS ne verront pas.

La liste des en-têtes d'extension possible est, depuis le RFC 7045, dans un registre IANA <https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#extension-header>. Dans un paquet IPv6, ces en-têtes sont organisés en une chaîne, chaque en-tête ayant un champ "*Next Header*" qui indique le type de l'en-tête suivant. La chaîne se termine par un en-tête du protocole de transport (typiquement TCP ou UDP), par un nouvel en-tête IPv6 (dans le cas d'une encapsulation IPv6-dans-IPv6), par un en-tête IPsec, ou bien par un en-tête dont le champ "*Next Header*" vaut 59, indiquant que rien ne le suit. Analyser cette chaîne est non trivial <https://www.bortzmeyer.org/analyse-pcap-ipv6.html>, mais c'est nécessaire pour le filtrage ou l'observation. Un pare-feu à qui

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2460.txt

on dit « tu bloques tout sauf les paquets TCP à destination des ports 22 et 80 » a besoin d'analyser la chaîne des en-têtes, puisqu'il doit arriver à l'en-tête TCP pour y trouver les numéros de ports. Et cet en-tête TCP n'est pas à une position fixe par rapport au début du paquet. Certains équipements de sécurité, par exemple des pare-feux, sont sans état : ils analysent chaque paquet indépendamment des autres, et n'essaient pas, par exemple, de reconstituer les datagrammes fragmentés. Si la chaîne des en-têtes est très longue, l'en-tête TCP peut se retrouver dans le deuxième fragment, ce qui va être très embêtant pour le pare-feu sans état (section 4 de notre RFC). Comme le premier fragment ne contient pas assez d'information pour décider, le pare-feu a deux choix : le bloquer, et il va alors filtrer un datagramme qui était peut-être légitime. Ou bien le laisser passer mais, pour accepter ou non les fragments suivants, le pare-feu a besoin de se souvenir de ce premier fragment, ce qui n'est pas possible sans garder un état.

D'où la nouvelle règle édictée par notre RFC, dans sa section 5 : **tous les en-têtes doivent être dans le premier fragment**. Si ce n'est pas le cas, les machines terminales devraient jeter le paquet en question (on a le droit de mettre une option de configuration pour les laisser passer quand même). Les machines intermédiaires (routeurs et pare-feux) ont le droit d'en faire autant.

Cette destruction du paquet invalide peut être accompagnée de l'émission d'un paquet ICMP, de type 4 ("*Parameter problem*") et de code 3 (ce nouveau code, "*First- fragment has incomplete IPv6 Header Chain*" a été ajouté dans le registre IANA <https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-3>).

On notera que la taille maximale d'une chaîne d'en-têtes dépend donc de la MTU. Si l'émetteur ne fait pas de découverte de la MTU du chemin, il doit se limiter à la taille minimale d'IPv6, 1 280 octets <https://www.bortzmeyer.org/fragmentation-ip-1280.html>.

Ce RFC fait partie des normes qui sont venues après la mise en œuvre : il existe déjà plusieurs pare-feux IPv6 sans état qui jettent sans merci les paquets lorsque la chaîne complète des en-têtes n'est pas entièrement dans le premier fragment.