

RFC 5095 : Deprecation of Type 0 Routing Headers in IPv6

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 Janvier 2008

Date de publication du RFC : Décembre 2007

<http://www.bortzmeyer.org/5095.html>

Ce RFC supprime un type particulier d'en-tête IPv6, qui permettait de faire du routage IP contrôlé par la source mais qui ouvrait la voie à de graves attaques par déni de service.

Normalement, le routage dans IP se fait uniquement en fonction de l'adresse de destination. Une technique connue sous le nom de « routage par la source » (*source routing*) permet de placer dans un paquet IP des instructions pour les routeurs situés sur le trajet, forçant l'usage d'un chemin particulier. En IPv4, ce routage par la source se fait en indiquant la route (les routeurs par lesquels le paquet doit passer) dans l'en-tête IP, où la taille est limitée. Cela limitait donc sérieusement l'utilité de ce routage par la source, mais aussi ses dangers, puisque un paquet ne pouvait pas être forcé sur un chemin très long. Néanmoins, cette option est tellement facile à utiliser pour contourner les politiques de sécurité, qu'elle est désactivée sur la plupart des routeurs IP (option `sysctl net.ipv4.conf.all.accept_source_route` sur Linux, par exemple ou bien `no ip source-route` sur IOS).

Mais la menace en IPv6 était plus sérieuse. En effet, l'en-tête IPv6 est de taille fixe et les options sont placées dans des en-têtes auxiliaires, qui sont très variés (section 4 du RFC 2460¹). Cela permet de mettre des en-têtes de très grande taille. L'un d'eux, l'en-tête de routage (*Routing Header*, section 4.4 du RFC 2460) de type 0, permet de lister un plus grand nombre de routeurs intermédiaire qu'en IPv4 (et on peut indiquer plusieurs fois le même routeur, permettant ainsi des parties de ping-pong entre les routeurs). C'est celui, qui, suite à un article <http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf> très médiatisé (souvent avec des exagérations ridicules) expliquant comment il pouvait être mal utilisé, et suite à l'analyse du RFC 4942, vient d'être déclaré abandonné. (La faille de sécurité avait été enregistrée sous le numéro CVE-2007-2242 <<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2242>>.)

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

Désormais, spécifie la section 3 de notre RFC 5095, une machine IPv6 doit ignorer les en-têtes de routage de type 0.

La section 4.2 couvre un problème intéressant, le risque que certains coupe-feux soient programmés de manière excessive pour rejeter tous les paquets ayant un en-tête de routage, même d'autres types (par exemple, le type 2 est utilisé par le RFC 3775). C'est une situation qui s'est déjà produite avec le soi-disant ping of death, où plusieurs administrateurs de coupe-feux ont bloqué complètement ICMP, alors que la vulnérabilité n'avait rien de spécifique à ICMP.

Notre RFC avertit donc qu'il ne faut pas surréagir : bloquer tous les paquets ayant un en-tête de routage empêcherait complètement le déploiement de beaucoup de protocoles.