# RFC 6980 : Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 août 2013

Date de publication du RFC : Août 2013

https://www.bortzmeyer.org/6980.html

---

Ce court RFC traite un problème de sécurité lorsqu'on combine la fragmentation avec le protocole NDP d'IPv6. Il interdit désormais cette combinaison, qui pouvait être exploitée pour des attaques sur le réseau local.

NDP est normalisé dans le RFC 4861 [1] (que ce RFC 6980 met à jour). Ce protocole est utilisé pour bien des choses, notamment pour résoudre une adresse IPv6 en adresse MAC et pour découvrir les routeurs du réseau local, ainsi que les préfixes des adresses IP de ce réseau (pour l'auto-configuration). Ses faiblesses de sécurité (très proches de celles d'ARP en IPv4) sont bien connues (RFC 3756). Notamment, n'importe quelle machine peut émettre des paquets NDP et répondre aux questions adressées à une autre machine. Ou bien l'attaquant peut se faire passer pour le routeur et émettre des « RAcailles », ces faux paquets RA ("*Router Advertisment*").

Il existe plusieurs moyens de gérer ces dangers. On peut mettre des ACL statiques dans les commutateurs, n'autorisant les RA que sur le port où se trouve le routeur. Ou bien on peut utiliser la solution un peu plus sophistiquée du "*RA guard*" (RFC 6105). On peut aussi surveiller le trafic, avec un IPS ou bien un logiciel comme NDPmon <http://ndpmon.sourceforge.net/> ou ramond <http://ramond.sourceforge.net/>, et lever une alarme lorsque quelque chose d'anormal se produit. Mais toutes ces techniques ont un défaut commun : elles reposent sur une analyse du paquet pour détecter si c'était du NDP et il est trop facile de les tromper en fragmentant le paquet. S'il est en deux parties, avec les informations permettant de reconnaître et d'analyser le NDP dans le deuxième paquet, aucun des systèmes existants ne voit ce qui se passe, alors que la machine terminale réassemblera le paquet et se fera donc avoir. À l'heure actuelle, la totalité des mises en œuvre de "*RA guard*" est ainsi

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4861.txt

vulnérable (cf. RFC 7113). Bien sûr, des outils comme les IPS pourraient réassembler les paquets eux-aussi, pour voir le paquet original, mais c'est plus difficile pour les commutateurs Ethernet. Et cela leur fait courir un risque (si l'attaquant génère des quantités de fragments afin d'épuiser la mémoire des réassembleurs, pour faire une attaque par déni de service).

C'est d'autant plus balot que les vrais paquets NDP sont rarement assez grands pour avoir réellement besoin de la fragmentation (section 2). Même si un routeur a besoin d'annoncer de nombreux préfixes dans ses RA, il peut le faire en plusieurs datagrammes IP, il n'est pas nécessaire de tout mettre dans un seul grand datagramme fragmenté. Bref, la fragmentation est quasi-inutile pour NDP alors qu'elle est dangereuse. (Une exception partielle est décrite en section 3, pour SEND, dans le RFC 3971, dans le cas où il y a des gros certificats à transmettre. Je ne la mentionne pas davantage puisque SEND n'est quasiment jamais utilisé. Il résout radicalement presque tous les problèmes de sécurité de NDP mais le manque de mises en œuvre de ce protocole, et la difficulté qu'il y a à distribuer les clés cryptographiques nécessaires font qu'en pratique, SEND n'est pas une approche envisageable. Voir la conférence de l'auteur à DEEPSEC <http://www.si6networks.com/presentations/deepsec2011/fgont-deepsec2011-ip
pdf>.)

La section 4 résume les raisons d'abandonner la fragmentation pour NDP :

— Il existe déjà des mises en œuvre d'IPv6 qui ignorent les paquets NDP fragmentés,
— Dans la vraie vie, comme expliqué en sections 2 et 3, les paquets NDP réels ne sont pas assez grands pour être fragmentés.

Donc, la section 5 du RFC expose la nouvelle règle, qui met à jour le RFC 4861 : **une machine qui émet des paquets NDP ne doit pas fragmenter ces paquets**. (Une exception partielle est faite pour les messages "*Certification Path Advertisement*" utilisés par SEND. Mais, pour tous les messages habituels, la règle est l'interdiction de la fragmentation.) À la réception, les paquets NDP fragmentés doivent être ignorés.

Si vous voulez créer vous-même de tels paquets NDP fragmentés (qui seront ignorés par les systèmes modernes, vous pouvez utiliser la boîte à outils SI6 présenté dans mon article sur le hacking IPv6 <https://www.bortzmeyer.org/hacking-ipv6.html>, avec l'option `-y`. Par exemple :

```
# ./ra6 -y 8  -i eth1 -d 2001:db8:8bd9:8bb0:ba27:ebff:feba:9094
```

va générer deux fragments, huit octets n'étant pas assez pour mettre le RA. tcpdump les voit ainsi :

```
08:34:29.122863 IP6 fe80::8609:88f4:14:a635 > 2001:db8:8bd9:8bb0:ba27:ebff:feba:9094: frag (0|8) ICMP6, rout
08:34:29.122883 IP6 fe80::8609:88f4:14:a635 > 2001:db8:8bd9:8bb0:ba27:ebff:feba:9094: frag (8|8)
```

Notez que tcpdump ne s'est pas laissé avoir : il a bien identifié le premier fragment comme appartenant à un RA.