RFC 9077 : NSEC and NSEC3: TTLs and Aggressive Use

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 juillet 2021

Date de publication du RFC : Juillet 2021

https://www.bortzmeyer.org/9077.html

Ce nouveau RFC corrige une légère bavure. Lorsqu'on utilise la mémorisation énergique du RFC 8198 [1] pour synthétiser des réponses DNS en utilisant les informations DNSSEC, les normes existantes permettaient une mémorisation pendant une durée bien trop longue. Cette erreur (peu grave en pratique) est désormais corrigée.

Rappelons que le principe du RFC 8198 est d'autoriser un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> à synthétiser des informations qu'il n'a normalement pas dans sa mémoire, notamment à partir des enregistrements NSEC de DNSSEC (RFC 4034, section 4). Si un résolveur interroge la racine du DNS :

```
%     dig @a.root-servers.net A foobar
...
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 37332
...
foo. 86400 IN NSEC food. NS DS RRSIG NSEC
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8198.txt

La réponse est négative (NXDOMAIN) **et** un enregistrement NSEC annonce au client DNS qu'il n'y a pas de nom dans la racine entre .foo et .food. Si le résolveur mémorise cette information et qu'on lui demande par la suite un nom en .foocat, il n'aura pas besoin de contacter la racine, il sait, en raison de l'enregistrement NSEC que ce nom ne peut pas exister.

Bon, mais combien de temps le résolveur peut-il mémoriser cette non-existence ? Le RFC 2308 disait qu'une réponse négative (NXDOMAIN) pouvait être mémorisée pendant une durée indiquée par le **minimum** du champ Minimum de l'enregistrement SOA et du TTL de ce même enregistrement SOA. Mais le RFC 4034, normalisant DNSSEC, disait que l'enregistrement NSEC devait avoir un TTL égal au champ Minimum du SOA. Dans l'exemple de la racine du DNS, à l'heure actuelle, cela ne change rien, ces durées sont toutes égales. Mais elles pourraient être différentes. Si un enregistrement SOA a un Minimum à une journée mais un TTL d'une heure, le RFC 2308 impose une heure de mémorisation au maximum, le RFC 4034 permettait une journée. . .Ça pourrait même être exploité pour une attaque en faisant des requêtes qui retournent des enregistrements NSEC, afin de nier l'existence d'un nom pendant plus longtemps que prévu. [Bon, dans le monde réel, je trouve que c'est un problème assez marginal mais ce n'est pas une raison pour ne pas le corriger.]

Le RFC 8198 avait déjà tenté de corriger le problème mais sans y réussir. Notre nouveau RFC impose désormais clairement que, contrairement à ce que dit le RFC 4034 (et deux ou trois autres RFC sur DNSSEC), la durée maximale de mémorisation est bien le **minimum** du champ Minimum de l'enregistrement SOA et du TTL de ce même enregistrement SOA.

Si les logiciels que vous utilisez pour signer les zones ne peuvent pas être corrigées immédiatement, le RFC demande que vous changiez le contenu de la zone pour mettre la même valeur au champ Minimum de l'enregistrement SOA et au TTL de ce même enregistrement SOA.

En pratique, les signeurs suivants ont déjà été corrigés :

— PowerDNS (par l'auteur du RFC) dans la version 4.3.0 (voir cette note dans la documentation <https://doc.powerdns.com/authoritative/dnssec/operational.html?highlight=ttl#some-notes-on-ttl-usage>).
— BIND dans la version 9.16 (voyez la correction <https://gitlab.isc.org/isc-projects/bind9/-/merge_requests/4506>, qui est très courte).
— Knot DNS dans la 3.1 (apparemment pas encore publiée, mais la correction <https://gitlab.nic.cz/knot/knot-dns/-/merge_requests/1219> a déjà été incluse).
— ldns <https://nlnetlabs.nl/projects/ldns/> dans une correction pas encore intégrée ? <https://github.com/NLnetLabs/ldns/pull/118>
— Pour les autres logiciels, une liste est en ligne <https://trac.ietf.org/trac/dnsop/wiki/draft-ietf-dnsop-nsec-ttl>.