RFC 9276 : Guidance for NSEC3 Parameter Settings

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 août 2024

Date de publication du RFC : Août 2022

https://www.bortzmeyer.org/9276.html

Si vous êtes responsable d'une zone DNS, et que vous la testez régulièrement avec des outils comme Zonemaster <https://zonemaster.fr/> ou DNSviz <https://dnsviz.net/> (ce que font tous les responsables sérieux), vous avez peut-être eu des avertissements comme quoi vos « paramètres NSEC3 » n'étaient pas ceux conseillés. C'est parce que les recommandations en ce sens ont changé avec ce RFC. Lisez-le donc si vous voulez comprendre les recommandations actuelles.

D'abord, un peu de contexte. Ce RFC concerne les zones qui sont signées avec DNSSEC **et** qui utilisent les enregistrements NSEC3 du RFC 5155[1]. Aujourd'hui, par exemple, c'est le cas de .fr, .com mais aussi de bortzmeyer.org grâce à qui vous êtes arrivés sur cet article. Mais ce n'est pas le cas de la racine des noms de domaine, qui utilise NSEC (RFC 4035). Pour comprendre la dfifférence entre les deux, je vous renvoie à mon article sur le RFC 5155.

Un exemple où Zonemaster <https://zonemaster.fr/> proteste, sur icann.org :

Ce RFC 5155 donnait des conseils de sécurité cryptographiques qui, avec le recul et l'expérience se sont avérés sous-optimaux. Ce nouveau RFC 9276 les modifie donc et suggère fortement de ne plus utiliser de sel, ni d'itérations successives, dans le calcul des condensats pour NSEC3.

Lorsqu'une zone est signée avec utilisation de NSEC3, elle comprend un enregistrement de type NSEC3PARAM qui indique quatre choses :

— L'algorithme de condensation utilisé (presque toujours SHA-1, aujourd'hui, c'est le seul normalisé <https://www.iana.org/assignments/dnssec-nsec3-parameters/dnssec-nsec3-parameters.xml#dnssec-nsec3-parameters-3>). Il n'est pas discuté ici (voir le RFC 8624 sur le choix des algorithmes).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5155.txt

— Les options, notamment celle nommée "*opt-out*" et qui est un avantage souvent oublié de NSEC3 par rapport à NSEC : la possibilité de ne pas avoir un enregistrement NSEC3 par nom mais seulement par nom signé. C'est un peu moins sûr (les noms non signés, typiquement les délégations DNS, ne sont pas protégés) mais ça fait une grosse économie de mémoire pour les zones qui comprennent beaucoup de délégations non signées (et cela évite de passer trop de temps à modifier les chaines NSEC3 dans des zones qui changent souvent). C'est typiquement la cas des gros TLD et cela explique pourquoi `.fr` ou `.com` utilisent NSEC3, même s'il n'y a pas de problème avec l'énumération des noms (`.fr` distribue la liste <https://opendata.afnic.fr/>). (Notez que si l'option est à 0 dans le NSEC3PARAM, cela ne signifie pas qu'il n'y a pas d'"*opt-out*", celui-ci est typiquement indiqué uniquement dans les enregistrements NSEC3.)
— Le nombre d'itérations **supplémentaires** (RFC 5155, sections 3.1.3 et 4.1.3) faites lorsqu'on condense un nom.
— Le sel utilisé.

Voici par exemple l'enregistrement de `icann.org` en août 2024 :

```
% dig +short icann.org NSEC3PARAM
1 0 5 A4196F45E2097176
```

Utilisation de SHA-1 (le 1 est le code de SHA-1), pas d'"*opt-out*" (mais prudence, son utilisation n'est pas obligatoirement signalée dans les options, voir plus haut), cinq itérations supplémentaires (donc six au total) et un sel apparemment aléatoire, `A4196F45E2097176`.

La première recommandation du RFC concerne le nombre d'itérations. Comme le sel, le but est de rendre plus difficile l'utilisation de tables calculées à l'avance par un attaquant. Sans sel et avec une seule itération, un attaquant qui a à l'avance calculé tout un dictionnaire et sait donc que le condensat de `foobar` est `8843d7f92416211de9ebb963ff4ce28125932878` pourra donc facilement inverser le condensat dans un enregistrement NSEC3. C'est pour cela que le RFC 5155 recommandait un nombre variable d'itérations, indiqué par l'enregistrement NSEC3PARAM. Mais, en pratique, la protection contre l'énumération n'est pas si solide que ça. Bien des noms peuvent être devinés (`www` étant le plus évident mais il y a aussi les mots d'un dictionnaire de la langue), d'autant plus qu'on choisit en général un nom de domaine pour être simple et facilement mémorisable <https://www.afnic.fr/observatoire-ressources/papier-expert/8-astuces-pour-bien-choisir-son-nom-de-domaine/>. Et que ces noms se retrouvent à plein d'endroits comme les journaux "*Certificate Transparency*" (RFC 9162). L'opinion d'aujourd'hui est que le jeu (la protection contre l'énumération) n'en vaut pas la chandelle (le coût de signature **et** de validation). Notez aussi une externalité négative : les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> aussi devront effectuer ces itérations et sont donc concernés. Bon, en prime, les techniques modernes rendent la protection peu efficace de toute façon (cf. « "*GPU-Based NSEC3 Hash Breaking*" <https://doi.org/10.1109/NCA.2014.27> »). La recommandation du RFC est donc de ne pas avoir d'itérations supplémentaires, donc de mettre ce nombre à zéro.

Et la deuxième recommandation concerne le sel. Il y a dans NSEC3 un sel implicite, c'est le nom de domaine (RFC 5155, section 5). D'ailleurs, mon exemple de condensat de "*foobar*" était faux, puisque j'avais omis cette étape. Si on l'inclut, le sel supplémentaire indiqué dans l'enregistrement NSEC3PARAM perd de son intérêt. En outre, en pratique, on change rarement le sel (cela nécessite de modifier toute la chaine NSEC3) ce qui diminue la protection qu'il offre. La recommandation actuelle est donc de ne pas utiliser de sel (ce qui se note avec un tiret, pas avec une chaine vide).

Si on suit les recommandations du RFC, le NSEC3PARAM aura cette allure :

```
% dig +short fr NSEC3PARAM
1 0 0 -
```

Et un des NSEC3 sera du genre :

```
% dig nexistesurementpas.fr
qu7kmgn3e....fr. 594 IN NSEC3 1 1 0 - (
                                QU7MMK1...
                                NS DS RRSIG )
```

Notez aussi que le RFC recommande (section 3), avant de réfléchir aux paramètres de NSEC3, de réfléchir à NSEC3 lui-même. Sur une grosse zone de délégation, changeant souvent, comme `.fr`, NSEC3 est tout à fait justifié en raison des avantages de l'"*opt-out*". Mais sur la zone DNS typique d'une petite organisation, qui ne compte souvent que des noms prévisibles (l'apex, `www` et `mail`), NSEC3 peut avantageusement être remplacé par NSEC, qui consomme moins de ressources. (NSEC3, ou d'ailleurs les couvertures minimales du RFC 4470, peut, dans le pire des cas, faciliter certaines attaques par déni de service.)

Les recommandations précédentes s'appliquaient aux signeurs de zone (côté serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>, donc). Mais la section 3 a aussi des recommandations pour les résolveurs : compte-tenu du coût que représente pour eux les itérations NSEC3, ils ont le droit d'imposer un maximum, et de le diminuer petit à petit. Ces résolveurs peuvent refuser de répondre (réponse SERVFAIL) ou bien traiter la zone come n'étant pas signée (cf. section 6). Un nouveau code d'erreur étendu (RFC 8914), le numéro 27 <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#extended-dns-error-codes>, "*Unsupported NSEC3 iterations value*", a été réservé pour qu'ils puissent informer leurs clients.

Revenons aux serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> : le RFC précise aussi qu'un hébergeur DNS devrait informer clairement ses utilisateurs des paramètres NSEC3 qu'il accepte. Il ne faudrait pas qu'on choisisse N itérations et qu'on s'aperçoive au déploiement qu'un des secondaires n'accepte pas d'en faire autant.

Aujourd'hui, la grande majorité des zones utilisant NSEC3 est passée aux recommandations de ce RFC (comme par exemple .fr en 2022 <https://www.afnic.fr/observatoire-ressources/papier-expert/rfc-9276-lafnic-adopte-le-regime-sans-sel/>). Notons que `.org` a un sel mais pas d'itérations supplémentaires.

```
 % dig +short org NSEC3PARAM
1 0 0 332539EE7F95C32A
```

Si vous utilisez OpenDNSSEC pour automatiser les opérations DNSSEC sur vos zones, voici la configuration conforme au RFC que j'utilise :

```
<Denial>
        <NSEC3>
                <!-- <OptOut/> -->
                <Resalt>P100D</Resalt>
                <Hash>
                        <Algorithm>1</Algorithm>
                        <Iterations>0</Iterations>
                        <Salt length="0"/>
                </Hash>
        </NSEC3>
</Denial>
```