La vulnérabilité DNS tsuNAME

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 mai 2021

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

L'Internet est plein de failles de sécurité donc, aujourd'hui, pas de surprise qu'une nouvelle faille soit publiée : tsuNAME <https://tsuname.io/> est une faille DNS permettant des attaques par déni de service en exploitant un cycle dans les dépendances des noms de domaine.

Le principe est simple : l'attaquant doit contrôler deux noms de domaine, avec un parent qui est la victime visée. Mettons que le méchant veuille attaquer le TLD `.example`, il a deux noms, `foo.example` et `bar.example`, il crée un cycle en faisant en sorte que les serveurs de noms de `foo.example` soient tous dans `bar.example` et réciproquement. En syntaxe de fichier de zone :

```
foo IN NS ns.bar.example.
bar IN NS ns.foo.example.
```

(C'est une présentation simplifiée : un attaquant peut faire des cycles plus complexes.) Aucun nom en `foo.example` ou `bar.example` ne peut être résolu avec succès, en raison de ce cycle. Mais le but de l'attaquant n'est pas là : lorsqu'un résolveur <https://www.bortzmeyer.org/resolveur-dns.html> veut résoudre `www.foo.example`, le serveur faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour `.example` le renvoie à `ns.bar.example`. Pour résoudre ce nom, il interroge à nouveau le pauvre serveur faisant autorité pour `.example`, qui le renvoie à `ns.foo.example` et ainsi de suite. (Si vous aimez les vidéos, je vous renvoie à celle de l'Afnic sur le fonctionnement du DNS <https://www.afnic.fr/observatoire-ressources/actualites/lafnic-met-en-ligne-une-video-sur-les-coulisses-des-noms-de-domaine/>.) Et, pire, certains résolveurs ne se souviennent pas que la résolution a échoué et recommencent donc la fois suivante. Un attaquant qui a configuré le cycle (ou bien repéré un cycle existant) peut donc utiliser les résolveurs auxquels il a accès (directement, ou bien via un botnet qu'il contrôle) pour faire l'attaque à sa place.

Normalement, les résolveurs limitent le nombre de requêtes déclenchées par une requête originale. Ils le font surtout pour se protéger eux-mêmes, par exemple contre les attaques en récursion infinie <https://www.ssi.gouv.fr/actualite/vulnerabilite-dns-critique-attaque-en-deni-de-service->. Mais la nouveauté de tsuNAME est de se servir d'un éventuel manque de limites pour attaquer les serveurs faisant autorité. En pratique, peu de résolveurs sont assez imprudents pour être vraiment intéressants pour l'attaquant. La principale exception était Google Public DNS, qui a ainsi involontairement participé à une attaque contre le `.nz`. (Il a été corrigé depuis.)

Une leçon pour les programmeurs de résolveurs DNS : ne vous laissez pas entrainer dans des cycles, pensez à jeter l'éponge rapidement, et à mémoriser cet échec pour la prochaine fois.