Vulnérabilité du DNS rendant l'empoisonnement plus facile

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 juillet 2008. Dernière mise à jour le 22 juillet 2008

http://www.bortzmeyer.org/faille-dns-empoisonnement.html

Le 8 juillet, l'avis VU#800113 <http://www.kb.cert.org/vuls/id/800113> du CERT a révélé publiquement une faille du protocole DNS. Cette faille permet un empoisonnement relativement facile des caches DNS.

On peut trouver un bon résumé dans l'article "*Fixes Released for Massive Internet Security Issue*" <http://securosis.com/publications/DNS-Executive-Overview.pdf>. L'attaque a été découverte par Dan Kaminsky et repose sur une vulnérabilité classique du DNS. Le résolveur DNS (serveur récursif) accepte en effet une réponse si la question posée, le "*Query ID*" (RFC 1035 [1], section 4.1.1) et le port UDP où arrive la réponse coïncident avec une question en attente. Mais Kaminsky a découvert un mécanisme pour envoyer une fausse réponse ayant de très bonnes chances d'être acceptée. (Le mécanisme détaillé est expliqué dans un autre article <http://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>.) Indépendamment de cette attaque spécifique, il faut noter que la vulnérabilité est connue depuis longtemps (voir par exemple l'article "*DNS and BIND Security Issues*" <http://www.usenix.org/publications/library/proceedings/security95/vixie.html> de Paul Vixie qui dit "*With only 16 bits worth of query ID and 16 bits worth of UDP port number, it's hard not to be predictable. A determined attacker can try all the numbers in a very short time and can use patterns derived from examination of the freely available BIND code. Even if we had a white noise generator to help randomize our numbers, it's just too easy to try them all.*") C'est pour cela que certains résolveurs ne sont pas vulnérables (ils mettaient en œuvre des mécanismes de défense depuis longtemps).

Depuis le site Web de l'auteur de la découverte <http://www.doxpara.com/>, on peut tester la vulnérabilité de son résolveur. Mais ledit site Web est très chargé et le code Javascript bogué. Si on veut tester via le Web, il faut mieux utiliser <https://www.dns-oarc.net/oarc/services/dnsentropy>. Si on préfère tester en local, une bonne solution est le script de Michael C. Toren (en ligne sur http://www.bortzmeyer.org/files/noclicky-1.00.pl) :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1035.txt

```
%  perl noclicky-1.00.pl 192.0.2.225
Looking up zqq0wi2odh5x.toorrr.com against 192.0.2.225
Fetching http://209.200.168.66/fprint/zqq0wi2odh5x
Requests seen for zqq0wi2odh5x.toorrr.com:
  192.0.2.225:32769 TXID=2234
  192.0.2.225:32769 TXID=22512
  192.0.2.225:32769 TXID=17521
  192.0.2.225:32769 TXID=32880
  192.0.2.225:32769 TXID=40914
Your nameserver appears vulnerable; all requests came from the same port.
```

Aïe, cette machine est vulnérable.

Et une autre solution pour tester la vulnérabilité de son serveur récursif, ne nécessitant que le traditionnel dig, est de demander à `porttest.dns-oarc.net` :

```
%  dig +short porttest.dns-oarc.net TXT
z.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"192.0.2.248 is POOR: 26 queries in 4.5 seconds from 1 ports with std dev 0.00                "
```

On voit que cette machine est vulnérable : toutes les requêtes DNS sont émises depuis le même port.

Enfin, deux autres outils plus graphiques, entièrement via le Web, et que je recommande, DNS ENtropy, de l'OARC <https://www.dns-oarc.net/oarc/services/dnsentropy> et le test de GRC <https://www.grc.com/dns/dns.htm>.

Les logiciels peuvent diminuer leur vulnérabilité en utilisant un port source UDP aléatoire. C'est ce que font toutes les mises à jour qui viennent d'être publiées (voir par exemple communiqué de l'ISC <http://www.isc.org/index.pl?/about/press/?pr=2008070800>). Le seul fait de choisir le "*Query ID*" au hasard est nécessaire mais pas suffisant (il ne fait que 16 bits de large). Certains résolveurs comme PowerDNS ou bien Unbound avaient déjà ce mécanisme et n'étaient donc pas vulnérables (pour Unbound, voir leur analyse complète <http://unbound.nlnetlabs.nl/pipermail/unbound-users/2008-July/000133.html> et aussi celle de PowerDNS <http://blog.netherlabs.nl/articles/2008/07/09/some-thoughts-on-the-recent-dns-vulnerability>).

Attention : il ne suffit pas de faire la mise à jour du logiciel, encore faut-il tester que la configuration du serveur de noms ne force pas l'usage d'un port unique. C'est par exemple un problème possible avec BIND si le fichier `named.conf` contient une ligne du genre `query-source port 53;`. Cette ligne, qui force l'usage d'un port unique annule tout l'effet du "*patch*" correctif ! (Et c'est détecté par les tests ci-dessus.)

Ces méthodes sont décrites dans un "*Internet-Draft*" nommé "*Measures for making DNS more resilient against forged answers*" <http://tools.ietf.org/id/draft-ietf-dnsext-forgery-resilience>.

Les systèmes comme Debian ou Gentoo ont très vite intégré les "*patches*" et la mise à jour normale suffit donc.

On peut noter que ce "*patch*" peut perturber certains coupe-feux, qui s'étonneraient des réponses arrivant à un grand nombre de ports. Par exemple, il semble que Zone Alarm sur Windows XP proteste et qu'il faille passer son niveau de sécurité à "*Medium*" si la machine fait tourner un BIND sécurisé (voir

<http://www.pcinpact.com/actu/news/44747-zonealarm-windows-dns-internet-probleme.htm> et <http://www.zdnet.fr/actualites/informatique/0,39040745,39382271,00.htm>.

Comme le rappelle le communiqué de l'ISC cité plus haut, la solution idéale est de passer à DNSSEC (RFC 4033, RFC 4034 et RFC 4035). Mais c'est une opération très lourde, nécessitant des mise à jour des logiciels, l'action des registres, celle des gérants de résolveurs, etc. Et DNSSEC apporte ses propres vulnérabilités et la complication de gestion qui est associé aux systèmes utilisant la cryptographie. Réclamer son déploiement est donc assez yakafokon.

Parmi les bonnes lectures sur le sujet, citons <http://sid.rstack.org/blog/index.php/283-dns-dns-dns>, <http://bruno.kerouanton.net/blog/2008/07/10/vous-avez-fini-de-patcher-ssh-patchez-vos-dn> ou <http://david.monniaux.free.fr/dotclear/index.php/2008/07/13/229-trou-du-dns>.

---

http://www.bortzmeyer.org/faille-dns-empoisonnement.html