# Même les systèmes de censure ont des bogues

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 juin 2025

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

---

Le dispositif de censure de l'Internet en Chine comprend de nombreux composants. L'un d'eux est une injection de fausses réponses DNS par des équipements réseau (et pas, comme c'est courant en Europe <https://labs.ripe.net/author/stephane_bortzmeyer/dns-censorship-dns-lies-as-seen-by-r>, par un résolveur <https://www.bortzmeyer.org/resolveur-dns.html> menteur). Comme tout logiciel, il a des bogues, et même des bogues menant à des failles de sécurité. C'est le cas de Wallbleed <https://gfw.report/publications/ndss25/en/>, une intéressante bogue, étudiée dans un article détaillé <https://www.ndss-symposium.org/ndss-paper/wallbleed-a-memory-disclosure->. Cette bogue permet d'observer plusieurs choses sur le système de censure chinois, par exemple ses pratiques de correction des bogues.

Prenons l'article <https://gfw.report/publications/ndss25/en/> dans l'ordre et sautons l'avertissement éthique ajouté par les organisateurs de la conférence NDSS <https://www.ndss-symposium.org/> (nous y reviendrons plus tard). D'abord, un petit rappel sur le fonctionnement du GFW, le "*Great Firewall of China*". En dépit de ce que pourrait faire croire ce terme journalistique, il n'y a pas un dispositif unifié mais un ensemble de dispositifs visant à empêcher le citoyen de base de s'informer ou de témoigner. C'est techniquement très efficace : si un des dispositifs est contournable, les autres pourront quand même censurer. Un de ces dispositifs est la génération de fausses réponses DNS. Rien à voir avec les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> menteurs. Ici, la fausse réponse est générée par un équipement du réseau qui, observant une requête DNS pour un nom censuré, envoie une réponse mensongère, avant celle du vrai serveur. Pas besoin d'aller en Chine pour tester ce dispositif, il suffit d'écrire à une adresse IP située en Chine, même si elle n'a pas de serveur DNS actif (puisque la réponse est fabriquée par le réseau). Essayons un nom non censuré, puis un nom censuré :

```
 % dig @113.113.113.113 coca-cola.com
;; communications error to 113.113.113.113#53: timed out
...
;; no servers could be reached

% dig @113.113.113.113 rsf.org

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @113.113.113.113 rsf.org
...
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10926
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
rsf.org.  73 IN A 108.160.162.98

;; Query time: 209 msec
;; SERVER: 113.113.113.113#53(113.113.113.113) (UDP)
;; WHEN: Wed Jun 11 10:38:28 CEST 2025
;; MSG SIZE  rcvd: 52
```

On le voit, bien qu'aucun serveur DNS n'existe sur `113.113.113.113` (qui est chez China Telecom), la censure a fabriqué une fausse réponse pour `rsf.org` (l'adresse IP renvoyée, qui est chez Dropbox, n'a aucun rapport avec RSF et ne répond pas).

C'est dans le code de la machine qui génère cette fausse réponse que se situe la bogue Wallbleed. Pour la comprendre, un petit mot sur le format des paquets DNS (vous avez tous les détails dans le RFC 1034[1], section 3.1 et le RFC 1035, section 4.1). Les noms de domaine dans le paquet ne sont **pas** représentés avec des points mais sous la forme d'un octet indiquant la taille du composant qui suit. `rsf.org` va être représenté par {3, r, s, f, 3, o, r, g, 0}. La forme texte n'est que pour les humains <https://www.bortzmeyer.org/representation-texte.html>. Conséquences pratiques : on peut mettre des points ou bien l'octet nul dans un nom de domaine, et c'est là-dessus que repose l'exploitation de la faille. (Il y a d'autres pièges dans l'analyse d'un paquet DNS, comme le fait que le nombre d'entrées dans chaque section peut être différent de la valeur indiquée dans l'en-tête DNS. Faites attention si vous écrivez du code. Les sections 3 et 4 du RFC 9267 détaillaient déjà des failles analogues à Wallbleed. Si un programme comme Drink <https://www.bortzmeyer.org/drink.html> a de nombreux tests d'analyse du paquet <https://framagit.org/bortzmeyer/drink/-/blob/master/test/drink_parsing_test.exs?ref_type=heads>, ce n'est pas pour rien.)

Car les auteurs du dispositif de censure n'ont pas lu le RFC 9267. Comme le montre les expériences des auteurs de l'article, leur logiciel commence par traduire la forme binaire du nom de domaine en texte, puis la teste contre les noms censurés, apparemment stockés sous forme d'une expression rationnelle (l'article explique bien comment les chercheurs ont découvert cela). Si on envoie un nom écrit sous la forme {3, r, s, f, 4, o, r, g, 0, 120...}, il va être traduit sous forme d'une chaine de caractères `rsf.org\000...`, interprétée par le programme comme étant `rsf.org` (le caractère nul étant pris comme la fin de la chaine dans leur programme, apparemment écrit en C) et va donc déclencher la génération de la réponse mensongère. Le programme va alors copier le nom demandé dans la réponse mais, pour cela, il se fiera à la longueur du nom en binaire, plus de 120 caractères (l'octet indiquant une longueur 120, mis par le client, donc l'attaquant). Et il copiera donc dans la réponse bien plus d'octets qu'il n'y en avait dans `rsf.org`, prenant ces octets dans sa mémoire et faisant ainsi fuiter ce qu'elle contenait. Le nom de la faille fait évidemment référence à Heartbleed, qui permettait également de récupérer des informations contenues dans la mémoire du serveur bogué. Si vous êtes programmeuse ou programmeur en C, l'article contient d'ailleurs une mise en œuvre du système de réponse, avec sa bogue, écrite par rétro-ingénierie, et qui permet de bien voir le problème.

Une fois cette faille découverte, les auteurs ont pu étudier plein de choses intéressantes. Par exemple, le fait que toutes les requêtes DNS passant par la Chine n'étaient pas vulnérables, cela dépendait du chemin suivi. Il y a donc apparemment plusieurs mises en œuvre du dispositif de censure par réponses

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc1034.txt`

DNS mensongères et toutes n'avaient pas la faille. De même, les auteurs ont pu étudier la correction de la bogue, en continuant à envoyer des paquets truqués : les responsables de la censure ont détecté la faille, et l'ont corrigé (en deux fois, la première correction ayant été insuffisante). À noter que certains réseaux chinois ont gardé la version boguée pendant plus longtemps, montrant que l'administration du dispositif de censure n'est pas centralisée.

Autre étude, qu'il y avait-il dans la mémoire de la machine de censure ? Apparemment du trafic réseau sans lien avec le DNS, indiquant que la machine de censure observait tout.

Cette étude est passionnante mais soulève plusieurs questions éthiques <https://labs.ripe.net/author/kistel/ethics-of-ripe-atlas-measurements/>, que l'article détaille :

— Les chercheurs récupèrent les données qui étaient dans la mémoire, et pouvaient donc obtenir des données sensibles,
— Les chercheurs exploitaient activement une faille de sécurité,
— Les chercheurs n'ont pas immédiatement prévenu le gouvernement chinois.

On l'a dit, ces questions éthiques ont mené à l'ajout dans l'article d'un avertissement très long (et qu'on voit très rarement dans ce genre d'articles), mis par les organisateurs de la conférence où la faille était publiée. Personnellement, je trouve que les auteurs de l'article ont très bien traité les problèmes éthiques et que ces organisateurs exagéraient beaucoup :

— Si quelqu'un envoyait en clair des données sensibles en Chine, il ne devait pas trop s'étonner que plein de gens les récupèrent,
— Le système de censure étant lui-même une attaque, le fait de l'≪ attaquer ≫ n'est pas si grave que ça,
— L'étude est très intéressante et utile et il est donc parfaitement normal de ne pas avoir prévenu tout de suite ; cette information du gouvernement chinois était prévue pour la fin de l'étude, mais, finalement, la faille a été découverte, apparemment de manière indépendante. (Les nombreux paquets envoyés par les chercheurs ont peut-être donné l'alerte.)