

2017 : la seconde de plus qui a débousolé

Cloudflare

Le passage de 2016 à 2017, qui s'est caractérisé par l'ajout d'une seconde afin de raccorder le temps astronomique (lié à la rotation de la Terre) à la mesure du temps standard, n'aura pas eu d'effet réellement visible sur les systèmes informatiques... Sauf chez Cloudflare. « *A minuit UTC (en temps universel, NDLR) le jour du Nouvel An, à l'intérieur du logiciel maison RRDNS de Cloudflare, un nombre est devenu négatif alors qu'il aurait toujours dû être au moins égal à zéro* », écrit John Graham-Cumming, le directeur technique du prestataire spécialisé dans la lutte anti-DDoS, dans un [billet](#) de blog. Avec un effet relativement limité si on en croit le responsable, qui parle d'un faible taux d'erreurs dans les résolutions DNS opérées par le prestataire pour ses clients. « *Au pic de la panne, environ 0,2 % des requêtes DNS étaient concernées et moins de 1 % des requêtes HTTP vers Cloudflare aboutissaient à une erreur* », précise le directeur technique. Selon le prestataire, le problème a été rapidement identifié et un correctif a été déployé dans la foulée. L'incident a été déclaré clos à 6h45 UTC.

« La croyance qu'on ne peut pas remonter le temps »

Reste la cause elle-même du dysfonctionnement, logée dans l'option CName. Via cette dernière, le service de résolution DNS de Cloudflare permet à ses clients de déclarer une redirection vers des alias de site plutôt que des renvois directs vers une adresse IP. Mais le CName oblige RRDNS à interroger les résolveurs DNS que fait tourner Cloudflare pour rechercher l'adresse IP finale. Ce sont certaines de ces résolutions DNS qui, durant le fameux saut d'une seconde, ont enregistré des valeurs négatives, débousolant l'application RRDNS.

« *La cause du bug qui a touché notre service DNS réside dans la croyance qu'on ne peut pas remonter le temps, détaille John Graham-Cumming. Dans notre cas, un morceau de code tenait pour garanti le fait que la différence entre deux temps serait toujours, à minima, zéro.* » Avec des résolveurs DNS tournant en quelques millisecondes, ce choix s'est avéré fatidique lors de l'ajout de la fameuse seconde, le temps où la requête était résolue pouvant alors se révéler inférieur au temps où cette dernière était émise. Générant une différence inférieure à zéro dans RRDNS. La présence de ces nombres négatifs dans l'application a eu des effets de bord, ces paramètres étant ré-exploités dans d'autres calculs, précise le CTO.

A lire aussi :

[DDoS : la menace de moins en moins fantôme](#)

[Dyn submergé par un botnet de 100 000 objets connectés](#)

[Failles NTP : la machine à détraquer le temps menace aussi le chiffrement](#)

Photo via [Visualhunt](#)