Sécurité des logiciels peu utilisés

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 mars 2009

https://www.bortzmeyer.org/securite-logiciels-peu-utilises.html

---

La publication récente de deux failles de sécurité dans le logiciel djbdns met l'accent sur un problème particulier de la sécurité, la question des logiciels peu utilisés, qui intéressent peu de monde et n'ont donc guère de revues de sécurité, laissant ainsi leurs utilisateurs dans le noir, quant aux risques de leur logiciel.

Le serveur DNS djbdns avait connu une petite période de popularité il y a pas mal d'années, lorsque BIND semblait la seule alternative. Aujourd'hui, il est bien dépassé (surtout par rapport à des logiciels modernes comme nsd ou Unbound <https://www.bortzmeyer.org/unbound.html>) et ne bénéficie donc pas de l'attention des experts en sécurité, qui travaillent sur des cibles qui leur apporteront davantage de gloire.

Néanmoins, il existe de temps en temps des analyses de sécurité de djbdns et deux ont été publiées coup sur coup, "*djbdns¡=1.05 lets AXFRed subdomains overwrite domains*" <http://article.gmane.org/gmane.network.djbdns/13864> et la plus sérieuse "*djbdns has two weaknesses that allow an attacker to poison its cache in very short amounts of time*" <http://www.your.org/dnscache/>. Elles ont montré que djbdns, en dépit de l'aggressivité de son auteur, avait sa part des failles de sécurité. Mais, par rapport à la longue liste des failles de sécurité de BIND, djbdns assure plutôt bien. Pourquoi ?

Le record du plus grand nombre de bogues publiées va t-il toujours au logiciel plus utilisé ? Microsoft a largement utilisé cet argument pour justifier leur catastrophique bilan en matière de sécurité. Mais il n'est pas forcément correct. Après tout, IIS (cf. le moteur de recherche de Microsoft <http://www.microsoft.com/technet/security/current.aspx>) a beaucoup plus d'alertes de sécurité qu'Apache (cf. "*Apache Security Vulnerabilities*" <http://httpd.apache.org/security_report.html>), bien que nettement moins utilisé <http://survey.netcraft.com/Reports/200903/>.

En fait, la principale différence n'est pas entre les logiciels très utilisés et ceux moins courants (il y a suffisamment de chercheurs en sécurité pour s'occuper également des challengers comme IIS pour les serveurs HTTP ou KDE pour le bureau). Mais certains logiciels sont tellement « en dessous du radar » qu'ils n'ont quasiment jamais de revues de sécurité. Si echoping <http://echoping.sourceforge.net/> n'a jamais eu d'alerte de sécurité depuis le début, je ne me fais pas d'illusion, ce n'est pas qu'il est particulièrement robuste, c'est parce que c'est un programme très peu connu.

Donc, pour résumer, si l'argument de Microsoft est mensonger, cela ne veut pas dire pour autant que tous les logiciels bénéficient de la même attention de la part des experts. Avant de vous vanter « mon logiciel n'a aucune faille de sécurité », cherchez d'abord s'il a été audité...