Log4Shell, et le financement du logiciel libre

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 décembre 2021

https://www.bortzmeyer.org/log4shell.html

Vous avez sans doute suivi l'affaire de la faille de sécurité Log4Shell. Elle a souvent été utilisée comme point de départ pour des discussions à propos du financement du logiciel libre, en mode « de nombreuses grosses entreprises utilisent tel logiciel libre et en dépendent mais ne contribuent pas à son financement ». Ce point de vue mérite d'être nuancé.

La faille concerne le logiciel Log4j, très utilisé (ce qui explique en partie l'intérêt porté à la faille Log4Shell). Comme beaucoup de logiciels libres très utilisés, il ne bénéficie pas d'une équipe de développeurs payés à temps plein pour le maintenir. Je cite tout de suite le dessin de XKCD que tout le monde mentionne tout le temps <https://xkcd.com/2347/>. Face à cela, on lit souvent des affirmations comme quoi les grosses entreprises (par exemple les GAFA) devraient financer ces logiciels cruciaux. Je pense que c'est plus compliqué que cela, et je voudrais présenter ici deux faits et une opinion.

Premier fait, un ou une développeureuse de logiciel libre n'est pas forcément bénévole. Le logiciel libre n'est pas synonyme de gratuité et, de toute façon, la gratuité du logiciel ne veut pas dire que les développeureuses n'ont pas été payé·es. Il y a beaucoup de logiciels libres cruciaux qui sont maintenus par des salarié·es. (Dans le domaine du DNS, c'est le cas de tous les serveurs libres, comme BIND ou NSD, maintenus par les employé·es de l'ISC, de NLnet Labs, de PowerDNS, etc.) D'affirmer comme je l'ai lu souvent qu'il faut s'inquiéter des logiciels libres car leurs développereuses sont bénévoles est donc absurde. La question du financement du logiciel libre est une question très intéressante (il est parfaitement normal que les programmeureuses soient payé·es pour leur travail) mais elle a de nombreuses réponses.

Deuxième fait, si le logiciel est libre, par définition, personne n'est **obligé** de payer pour l'utiliser. Du point de vue moral, on peut trouver que ce n'est pas beau qu'Amazon ou Google ne dépensent pas un centime pour des logiciels qu'ils utilisent mais c'est le principe du logiciel libre. Un·e auteur·e de logiciel peut toujours mettre son logiciel sous une licence non-libre, imposant par exemple un paiement pour un usage commercial (ce qui est en général une mauvaise idée <https://www.bortzmeyer.org/non-commercial.html>) mais ce n'est plus du logiciel libre.

Enfin, mon opinion. À défaut d'imposer un paiement, ce qui n'est pas possible pour un logiciel libre, ne faudrait-il pas au moins exercer une pression morale pour que les entreprises qui gagnent de l'argent avec une infrastructure composée en (bonne) partie de logiciel libre mettent la main sur l'interface Web de leur banque et envoient de l'argent ?

Ce point soulève de nombreuses questions. D'abord, si la programmeuse ou le programmeur a choisi le logiciel libre (et donc de ne pas forcément toucher de l'argent des utilisateurs), c'est qu'il y a une raison. Souvent, c'était pour être elle-même ou lui-même plus libre, pour ne pas dépendre de "*product owners*", de commerciaux ou de décideurs qui lui diraient qu'ils veulent telle ou telle jolie fonction dans l'interface. Si le financement des logiciels libres est assuré par des grosses entreprises, elles exigeront sans doute du "*reporting*", des "*process*" formalisés, elles demanderont un pouvoir de décision, et tou·tes les auteur·es de logiciel libre n'ont pas envie de travailler dans un tel cadre. Même si Amazon voulait payer, tout le monde ne le voudrait pas. (En outre, se faire payer pour développer du logiciel libre est parfois compliqué, du point de vue administratif, même si quelqu'un veut le faire.)

C'est d'autant plus vrai que ces grosses entreprises ont souvent un rôle très néfaste dans l'Internet. Je me souviens d'une discussion il y a quelques années avec la responsable d'un gros projet libre, financé en grande partie par des contrats avec des entreprises de l'Internet qui payaient pour que telle ou telle fonction soit développée. Je lui suggérai des améliorations pour préserver la vie privée des utilisateurices. Elle m'avait répondu « Stéphane, tu nous demandes toujours des trucs pour mieux protéger la vie privée, mais les clients qui paient nous paient pour, au contraire, trouver des moyens de récolter davantage de données. »

Bien sûr, une solution possible serait d'isoler les programmeuses ou programmeurs des financeurs via, par exemple, une fondation qui recevrait l'argent et le distribuerait (un certain nombre de gros logiciels libres fonctionnent ainsi, et c'est d'ailleurs le cas de Log4j). Mais cela ne convient pas non plus à tout le monde. (Ces fondations ne sont pas forcément innocentes <https://www.protocol.com/enterprise/linux-foundation-open-source-enterprise>.)

Et la sécurité n'y gagnerait pas forcément. Dans le cas de Log4Shell, les auteurs ont commis une bogue, c'est sûr. Mais tous les logiciels peuvent avoir des bogues, que leurs auteurs soient payés ou pas. Et, une fois la bogue signalée, tout semble indiquer que les auteurs de Log4j ont réagi vite et bien <https://twitter.com/yazicivo/status/1469349956880408583>. Tout n'est pas une question de financement, et, en matière de sécurité, la conscience professionnelle et la réactivité comptent davantage. Rajouter des règles, des procédures et de la bureaucratie, sous couvert d'avoir des dévelopements logiciels « plus sérieux » ne serait pas un progrès en sécurité, probablement plutôt le contraire. (Sans compter que les grosses entreprises sont les premières à réclamer davantage de fonctions, donc davantage de failles de sécurité, et à prioriser l'apparence sur la qualité.)

[Ne me faites pas dire ce que je n'ai pas dit ; je n'ai pas proposé que les développeur·ses de logiciels soient forcément pauvres et grelottant de froid dans une mansarde non chauffée. Qu'ielles soient payé·es est normal. Mais, vu l'actuel marché de l'emploi dans la programmation, celles et ceux qui ne s'intéressent qu'à l'argent n'ont en général pas de problème <https://www.zdnet.fr/blogs/zapping-decrypte/salaries-de-la-tech-continuez-de-demander-des-salaires-stratospheriq
htm>. La question du financement et de la maintenance des logiciels essentiels est importante, mais elle ne se résoudra pas en demandant simplement aux GAFA de mettre la main à la poche.]

Quelques lectures sur ce sujet délicat :

— Un appel à financer les développeurs dont on utilise le travail <https://lehollandaisvolant.net/?d=2021/12/12/15/01/11-log4shell-soutenez-les-dev-dont-vous-utilisez-le-trava
(appel qui n'est pas destiné qu'aux « grosses entreprises »).

— Un rappel de la situation dans Next Inpact <https://www.nextinpact.com/article/49180/log4shell-derriere-importante-faille-eternelle-question-soutien-au-logiciel-libre>.
— Un avis d'un employé de Google <https://blog.filippo.io/professional-maintainers/>, qui pointe entre autres les contraintes liées aux grandes entreprises, et qui illustre parfaitement les dangers dont je parle plus haut (en disant explicitement que de payer les développeureuses permettra de leur donner des ordres).
— Un article de Numérama <https://www.numerama.com/tech/789245-limmense-faille-log4shell-ra> décrit bien l'opinion dominante (« il faut faire payer les grosses entreprises »).
— Au contraire, cet article <https://www.haskellforall.com/2021/12/funding-isnt-problem-with-op> pointe les dangers du financement par les grosses entreprises.
— Un excellent article de Daniel Stenberg <https://daniel.haxx.se/blog/2022/01/17/enforcing-the-py> sur le sujet, pointant entre autres les difficultés paperassières à toucher de l'argent, même quand une entreprise ou l'État veut vous en donner, et également le fait que ce n'est pas un hasard si les logiciels touchés sont souvent des logiciels d'infrastructure, sans jolie interface que les décideurs peuvent admirer.
— Un développeur qui pointe la paperasserie nécessaire <https://nadim.computer/posts/2021-12-12-maintainers.html> pour se faire payer.
— Dans le débat, des gens disent souvent "*open source*" au lieu de logiciel libre, par snobisme, parce que c'est mieux en anglais (ou bien parce qu'ils ne comprennent pas le sujet). C'est pareil <https://www.bortzmeyer.org/free-software-open-source.html>.