Vente de vulnérabilités logicielles ; vrai ou pas vrai ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 mai 2014

https://www.bortzmeyer.org/ventes-vuln.html

Normalement, les gens qui découvrent une faille de sécurité dans un logiciel préviennent les mainteneurs du logiciel et ne publient qu'après avoir laissé du temps à ceux-ci de corriger la faille. C'est ce qu'on nomme le « "*responsible disclosure*" » (publication responsable). Évidemment, tout le monde n'est pas un être humain civilisé, il y a aussi des agents secrets qui gardent l'information pour que leur État puisse attaquer les autres, et il y a des pourris qui vendent ce genre d'informations à quiconque paiera. Question intéressante : avant d'acheter, comment on sait que la vulnérabilité est réelle ?

Un cas d'école récent est apparu le 30 avril. Un anonyme olckrrii3@openmailbox.org a envoyé un message sur Pastebin prétendant qu'il avait trouvé une faille dans OpenSSH permettant la lecture de la mémoire du serveur (comme Heartbleed permettait de lire la mémoire d'un serveur TLS). Il appuie ses dires par des transcriptions d'une exploitation de la faille, avec affichage de la mémoire du serveur. Le message est toujours sur Pastebin <http://pastebin.com/raw.php?i=gjkivAf3>, mais, s'il disparait, j'en ai une copie ici (en ligne sur https://www.bortzmeyer.org/files/vente-sshd-leak.txt) (ce qui ne signifie **pas** que je soutienne cette démarche). L'auteur du message réclame 20 bitcoins pour révéler la faille (soit dans les 6 300 € au cours actuel, ce qui est plutôt bon marché pour une faille aussi grave dans un logiciel aussi répandu).

La question à 20 bitcoins : est-ce que ce message est véridique ? A-t-il vraiment découvert une faille ou bien le succès médiatique de Heartbleed lui a-t-il simplement donné des idées ? La réponse est simple : il n'y a **aucun** moyen de le savoir. Ce qu'il affiche dans son message a pu être fabriqué de toutes pièces, le monde numérique ne permet pas de produire des preuves en enregistrant une session...

La seule ressource des gens qui veulent vérifier ces affirmations est de regarder le message et de voir s'il est cohérent. La grande majorité des tentatives précédentes étaient grossières (comme la grande majorité des spams sont ridicules et ne peuvent tromper que les gogos les plus naïfs). Il était facile d'y relever des incohérences ou des invraisemblances, qui ruinaient tout l'édifice (par exemple, une bannière SSH annonçant une Debian alors que le reste de l'attaque montrait une machine Fedora). Mais, si je parle du message de olckrrii3@openmailbox.org, c'est parce qu'il a été composé avec bien plus de soin que d'habitude. Il prétend avoir un numéro CVE, il donne les numéros de version exacts des logiciels testés, il affiche un "*dump*" mémoire convaincant... Tout cela a pu être fabriqué (et l'a probablement

été) mais cela lui a pris plus de cinq minutes, contrairement à la plupart de ces escroqueries. Résultat, son annonce a été relayée par pas mal de gens, attirés par le côté sensationnel de l'annonce (« *"Major Heartbleed-like vulnerability in OpenSSH!"* »).

Certaines personnes ont relevé des choses étonnantes dans le message (le programme d'exploitation qui pèse 236 ko, ce qui est énorme pour un client C d'attaque typique, sauf s'il contient du code généré automatiquement, ou un "*blob*" binaire) ou des incohérences (la taille du répertoire est inférieure à celle de l'unique fichier qu'il contient) mais cela n'est pas une preuve formelle, juste une indication. Bref, si on veut savoir, il faut être prêt à risquer ses 20 bitcoins... (Personne ne l'a encore fait, comme on peut le voir dans la blockchain Bitcoin `<https://blockchain.info/address/14PEL35LQf81oCvSPurhoyTSvosvtQT7u3>`, me rappelle Yan `<https://twitter.com/yangrunenberger>`.)

Le responsable d'OpenSSH a estimé que ce message était un faux `<http://www.pcworld.com/article/2151560/heartbleedlike-bug-in-openssh-dismissed-as-a-hoax.html>`. Si vous voulez acheter des vulnérabilités logicielles à un mercenaire, vous pouvez vous adresser à plusieurs sociétés à faible éthique comme le français Vupen `<http://www.vupen.com>` (« *"leading provider of defensive & offensive cyber security capabilities, advanced vulnerability research & government-grade zero-day exploits"* », se vante leur profil Twitter).