Ce que nous apprend Ghost au sujet des vieilles API

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 janvier 2015

https://www.bortzmeyer.org/ghost-getaddrinfo.html

Vous avez certainement déjà tout lu sur la vulnérabilité « Ghost » de la GNU libc (alias CVE-2015-0235 <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235>). Si ce n'est pas le cas, vous pouvez vous documenter sur le blog du découvreur <https://community.qualys.com/blogs/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability> ou bien en lisant cette analyse technique ultra-détaillée <http://www.openwall.com/lists/oss-security/2015/01/27/9>. Mais un aspect de cette faille a été peu remarqué : qui diable utilise encore l'API `gethostbyname`, complètement dépassée ?

La faille se trouvait en effet dans une fonction nommée `__nss_hostname_digits_dots` <https://sourceware.org/git/?p=glibc.git;a=blobdiff;f=nss/digits_dots.c;h=e007ef47a41b69437655c2656hp=2b862956e9a8c39bbccbea982add1d7ab2d16ab2;hb=d5dd6189d506068ed11c8bfa1e1e9bffde04decd;hpb=fef94eab0bd308d5059a2588c753bf9a4926845d> qui est appelée par les fonctions, bien plus connues, `gethostbyname` et `gethostbyaddr`. Ces fonctions servent à traduire un nom de domaine en adresse IP, en général en faisant appel au DNS. Elles sont dépassées depuis longtemps et ne devraient plus être utilisées, notamment parce qu'elles ne permettent pas de faire de l'IPv6.

Ce point a bien été noté par les découvreurs de la faille (et, indépendamment, par certains sur les rézosocios <https://twitter.com/bortzmeyer/statuses/560101323312726016>), auteurs qui notent, dans le rapport technique <http://www.openwall.com/lists/oss-security/2015/01/27/9>, « "*The gethostbyname*() functions are obsolete; with the advent of IPv6, recent applications use getaddrinfo() instead.*" ». En effet, en 2015, on n'imagine pas qu'il puisse exister des programmes qui se limitent volontairement à IPv4, en utilisant ces vieilles API.

Car ce n'est pas qu'une matière d'esthétique : les fonctions officiellement remplacées par des meilleures ne sont pas forcément aussi bien maintenues, et on peut penser que les failles n'y sont pas aussi vite repérées et corrigées. Les programmes utilisant les anciennes API ont donc plus de chance d'avoir des failles de sécurité comme Ghost.

Au fait, que faut-il utiliser depuis plus de quinze ans ? `getaddrinfo`, introduit à l'origine dans le RFC 2133 [1] et actuellement normalisé dans le RFC 3493. (Vous trouverez mes exemples personnels dans mon article sur les structures de données réseau en C <https://www.bortzmeyer.org/ip-data-structures.html>.) `gethostbyname` avait été marqué "*obsolescent*" dans POSIX en 2001 et supprimé complètement en 2008...

Aujourd'hui, si on cherche les « parts de marché » respectives de `gethostbyname` et `getaddrinfo`, on trouvera probablement qu'un grand nombre de programmes utilise toujours l'ancienne API. Ignorance, lecture de vieux HOWTO dépassés, cours jamais mis à jour...

Également à lire, sur Ghost :

— Un très bon exposé de Bert Hubert <http://ds9a.nl/har-presentation-bert-hubert-3.pdf> parlant entre autres de la qualité du code DNS de la GNU libc et des nombreuses bogues qui s'y cachent,
— Un article de Robert Graham <http://blog.erratasec.com/2015/01/you-shouldnt-be-using-get.html> qui dit la même chose que moi,
— Une excellente analyse technique de Ghost <http://lcamtuf.blogspot.fr/2015/01/technical-anal.html>.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2133.txt`