RFC 8270 : Increase the Secure Shell Minimum Recommended Diffie-Hellman Modulus Size to 2048 Bits

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 décembre 2017

Date de publication du RFC : Décembre 2017

http://www.bortzmeyer.org/8270.html

Un RFC de moins de quatre pages, "*boilerplate*" administratif inclus, pour passer la taille minimum des modules des groupes Diffie-Hellman utilisés par SSH, de 1 024 bits à 2 048.

L'échange Diffie-Hellman dans SSH est décrit dans le RFC 4419 [1], que notre nouveau RFC met à jour. C'est dans le RFC 4419 (sa section 3) que se trouvait la recommandation d'accepter au moins 1 024 bits pour le module du groupe. Or, cette taille est bien faible face aux attaques modernes comme Logjam.

Voilà, c'est tout, on remplace « minimum 1 024 bits » par « minimum 2 048 » et on peut continuer à utiliser SSH. Si vous êtes utilisateur d'OpenSSH, la commande de génération de clés, `ssh-keygen`, peut également générer ces modules (cf. la section "*Moduli generation*" dans le manuel.) Les versions un peu anciennes ne vous empêchent pas de faire des modules bien trop petits. Ainsi, sur une version 7.2 :

```
% ssh-keygen -G moduli-512.candidates -b 512
Fri Oct 20 20:13:49 2017 Sieve next 4177920 plus 511-bit
Fri Oct 20 20:14:51 2017 Sieved with 203277289 small primes in 62 seconds
Fri Oct 20 20:14:51 2017 Found 3472 candidates

% ssh-keygen -G moduli-256.candidates -b 256
Too few bits: 256 < 512
modulus candidate generation failed
```

Le RGS <https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/> recommande quant à lui 3 072 bits minimum (la règle exacte est « RègleLogp-1. La taille minimale de modules premiers est de 2048 bits pour une utilisation ne devant pas dépasser l[Caractère Unicode non montré [2]]année 2030. RègleLogp-2. Pour une utilisation au delà de 2030, la taille minimale de modules premiers est de 3072 bits. »)

Enfin, la modification d'OpenSSH pour se conformer à ce RFC est juste un changement de la définition de DH_GRP_MIN <http://freshbsd.org/commit/openbsd/2a2c1e4e7e3fcc787fa334f50347ee1d282fac45>

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4419.txt
2. Car trop difficile à faire afficher par LaTeX