RFC 8758 : Deprecating RC4 in Secure Shell (SSH)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 avril 2020

Date de publication du RFC : Avril 2020

https://www.bortzmeyer.org/8758.html

L'algorithme de chiffrement symétrique RC4, trop fragile, est abandonné depuis longtemps. Ce nouveau RFC le retire officiellement de SSH. Notre RFC remplace donc le RFC 4345 [1], dont le statut devient « Intérêt historique seulement ».

L'utilisation de RC4 dans SSH avait été enregistrée dans le RFC 4253, et précisée dans ce RFC 4345, désormais abandonné. Les faiblesses de RC4 sont connues depuis longtemps, et ont été documentées dans le RFC 7465. Résultat, RC4 est retiré peu à peu des protocoles Internet (cf. par exemple le RFC 8429.) Désormais, RC4 disparait également de SSH, et le registre IANA <https://www.iana.org/assignments/ssh-parameters/ssh-parameters.xml#ssh-parameters-17> des algorithmes a été mis à jour en ce sens.

OpenSSH a retiré RC4 il y a longtemps :

```
% ssh -V
OpenSSH_7.6p1 Ubuntu-4ubuntu0.3, OpenSSL 1.0.2n  7 Dec 2017

% ssh -Q cipher
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
rijndael-cbc@lysator.liu.se
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

(RC4 apparaissait comme `arcfour`, pour des raisons légales.)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4345.txt