RFC 4593 : Generic Threats to Routing Protocols

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 décembre 2006

Date de publication du RFC : Octobre 2006

https://www.bortzmeyer.org/4593.html

Parmi tous les risques de sécurité qui touchent Internet, notre RFC s'attache à décrire ceux qui visent les protocoles de routage.

Il n'y a pas d'analyse spécifique de chaque protocole. Celle pour BGP est déà fournie par le RFC 4272 [1]. Notre RFC, au contraire, décrit des attaques génériques, avec l'espoir que des solutions génériques puissent être développées.

Comme dans toute bonne analyse de sécurité, notre RFC commence par une analyse des attaquants, de leurs motivations et de leurs capacités. Puis il décrit les conséquences possibles des différentes attaques (du DoS jusqu'au détournement de trafic vers une machine qui pourra alors s'insérer dans une communication qui ne lui était pas destinée). Enfin, la section 4 en arrive aux actions du méchant : par exemple, la falsification des données de routage, pour annoncer des routes qu'il ne gère normalement pas.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4272.txt