RFC 8251 : Updates to the Opus Audio Codec

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 octobre 2017

Date de publication du RFC : Octobre 2017

https://www.bortzmeyer.org/8251.html

Le codec Opus, normalisé dans le RFC 6716 [1] a une particularité rare à l'IETF : il est spécifié par un programme, pas par une description écrite en langue naturelle. Les programmes ont des bogues et ce nouveau RFC corrige quelques petites bogues pas graves trouvées dans le RFC 6716.

C'est un vieux débat dans le monde de la normalisation : faut-il décrire un protocole ou un format par une description en langue naturelle (vecteur souvent ambigu) ou par une mise en œuvre dans un langage de programmation (qui fournira directement un programme utilisable), dans laquelle il sera difficile de distinguer ce qui est réellement obligatoire et ce qui n'est qu'un détail de cette mise en œuvre particulière ? Presque tout le temps, à l'IETF, c'est la voie de la description en anglais qui est choisie. Mais le RFC 6716, qui normalisait Opus, avait choisi une autre voie, celle du code source, écrit en C. C'est ce code qui est la loi.

Dans les deux cas, en anglais ou en C, les humains qui rédigent les normes font des erreurs. D'où ce RFC de correction, qui répare le RFC 6716 sur des points mineurs (la compatibilité est maintenue, il ne s'agit pas d'une nouvelle version d'Opus).

Chaque section du RFC est ensuite consacrée à une des erreurs. La section 3, par exemple, corrige un simple oubli dans le code de réinitialiser l'état du décodeur lors d'un changement. Le "*patch*" ne fait que deux lignes. Notez qu'il change le résultat produit par le décodeur, mais suffisamment peu pour que les vecteurs de test de l'annexe A.4 du RFC 6716 soient inchangés.

L'erreur en section 9 est également une erreur de logique dans la programmation. Sa correction, par contre, nécessite de changer les vecteurs de tests (cf. section 11).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6716.txt

Le reste des bogues, en revanche, consiste en erreurs de programmation C banales. Ainsi, en section 4, il y a un débordement d'entier si les données font plus de 2{}31-1 octets, pouvant mener à lire en dehors de la mémoire. En théorie, cela peut planter le décodeur (mais, en pratique, le code existant n'a pas planté.) Notez que cela ne peut pas arriver si on utilise Opus dans RTP, dont les limites seraient rencontrées avant qu'Opus ne reçoive ces données anormales. Cette bogue peut quand même avoir des conséquences de sécurité et c'est pour cela qu'elle a reçu un CVE, CVE-2013-0899 <https://nvd.nist.gov/vuln/detail/CVE-2013-0899>. Le "*patch*" est très court. (Petit rappel de C : la norme de ce langage ne spécifie pas ce qu'il faut faire lorsqu'on incrémente un entier qui a la taille maximale. Le résultat dépend donc de l'implémentation. Pour un entier signé, comme le type `int`, le comportement le plus courant est de passer à des valeurs négatives.)

Notez qu'une autre bogue, celle de la section 7, a eu un CVE, CVE-2017-0381 <https://nvd.nist.gov/vuln/detail/CVE-2017-0381>.

En section 5, c'est un problème de typage : un entier de 32 bits utilisé au lieu d'un de 16 bits, ce qui pouvait mener une copie de données à écraser partiellement les données originales.

Dans la section 6 du RFC, la bogue était encore une valeur trop grande pour un entier. Cette bogue a été découverte par "*fuzzing*", une technique très efficace pour un programme traitant des données externes venues de sources qu'on ne contrôle pas !

Bref, pas de surprise : programmer en C est difficile, car de trop bas niveau, et de nombreux pièges guettent le programmeur.

La section 11 du RFC décrit les nouveaux vecteurs de test rendus nécessaires par les corrections à ces bogues. Ils sont téléchargeables <https://www.ietf.org/proceedings/98/slides/materials-98-codec-tar.gz>.

Une version à jour du décodeur normatif figure désormais sur le site officiel <https://opus-codec.org/>. Le "*patch*" traitant les problèmes décrits dans ce RFC est en ligne <https://www.ietf.org/proceedings/98/slides/materials-98-codec-opus-update-00.patch>. Ce "*patch*" global est de petite taille (244 lignes, moins de dix kilo-octets, ce qui ne veut pas dire que les bogues n'étaient pas sérieuses).