OpenSSL met au jour sa politique d'annonces des vulnérabilités

OpenSSL, le projet Open Source de librairie de chiffrement, poursuit sa réorganisation. Après sa feuille de route de juin dernier, l'équipe met aujourd'hui à jour sa politique d'annonces de sécurité.

Rappelons que OpenSSL avait été mis sous les feux médiatiques après l'affaire Heartbleed, nom de la faille de sécurité qui touchait la librairie et pouvait exposer au grand jour, depuis plus de deux ans, les échanges de données chiffrées de **centaines de milliers de serveurs web** dans le monde. La faille avait permis de mettre en avant les aléas de certains projets de développement Open Source et avait poussé la Fondation Linux à lancer le projet Core Infrastructure Initiative visant à soutenir et améliorer le développement de logiciels Open Source massivement utilisés, dont OpenSLL. Le bénéfice de cette initiative se retrouve aujourd'hui dans la révision du mode de fonctionnement des développeurs de la librairie de chiffrement. Notamment à travers la publication de la politique de gestion de la sécurité, ce qui n'avait jamais été le cas jusqu'à peu.

Trois niveaux de sévérité des failles

Il n'y a pas d'originalité particulière à attendre en matière de **planification des divulgations de failles** qui adhère à la plupart des modèles d'annonces des éditeurs. *« Quand nous prévoyons une mise à jour qui corrige des problèmes de sécurité, nous en informons la liste de openssl-annoncer et mettons à jour la page d'accueil pour donner la date de notre mise à jour et la gravité des problèmes. Aucune autre information sur les problèmes ne sera communiquée »*, précise l'équipe de développement. De même, OpenSSL fait le choix d'assurer entièrement l'annonce des vulnérabilités. *« Nous avons précédemment utilisé des tiers pour s'occuper des notification pour nous, y compris CPNI, oCERT ou CERT//CC, mais aucun n'était*