Du rififi autour d'un module JavaScript bloque des milliers de projets

Ces dernières années, JavaScript est devenu un environnement de développement plus stable et mature. Oublié le temps où il fallait charger manuellement les librairies dans le code. Maintenant JavaScript est livré avec des gestionnaires des paquets des systèmes de build automatiques, tout comme Java, Ruby et d'autres langages de programmation plus matures.

Le gestionnaire de paquets JavaScript est npm. Il a débuté sa carrière au sein de Node.js, mais a ensuite été étendu pour couvrir tous les types de projets JavaScript. Or il y a eu un problème avec un petit module de npm baptisé left-pad et plus exactement avec son auteur, Azer Koçulu. Ce développeur est aussi à l'origine d'un autre module nommé Kik. Or les propriétaires de l'application mobile de chat Kik.com ont demandé au développeur de changer le nom du module. Dépôt de marque, risque de confusion, aucun argument n'a infléchi la position d'Azer Koçulu. Kik.com s'est donc retourné vers la direction de npm pour régler cela. Et son CEO, Isaac Z. Schlueter a accepté de renommer le module incriminée.

Une dépublication de l'ensemble des modules

Une initiative qui n'a pas été du goût de Azer Koçulu qui, sous le coup de la colère, a dépublié tous ses modules npm, les rendant disponibles uniquement sur GitHub. Parmi ces modules, il y a left-pad qui affiche 100 000 téléchargements quotidiens et 2,5 millions au cours du dernier mois. Surtout, il sert indirectement pour des projets comme ember, babel et react-native. Plusieurs projets ont été bloqués et pas mal de développeurs ont activé les débogages pour connaître la cause du problème.

Les réactions de la communauté ne sont pas faites attendre entre tweets de rage et discussions passionnées sur Reddit. De son côté, le développeur a expliqué dans son blog que « *cette aventure m'a fait réaliser que npm est un domaine privé où la direction est plus puissante que les gens et moi je fais de l'Open Source sur le modèle Power to people* ».

Retour à la normale, mais question sur la sécurité

Après son coup de sang, Azer Koçulu a accepté de transférer la propriété de ses projets à toute personne intéressée par sa prise en charge. Il a également accordé à npm la republication de ses modules, au plus grand soulagement des développeurs qui voient leur projet refonctionner. Mais en retirant ses modules, Azer Koçulu a également libéré les namespaces. Cela signifie que quelqu'un aurait pu enregistrer un autre module sous le nom left-pad et diffuser un code malveillant dans les build de milliers de projets JavaScript.

Un incident qui pose la question des faiblesses de l'Open Source, même si dans le cas présent, npm a pu rapidement republier une version antérieure de left pad et éviter que trop de projets tombent en carafe. Il met surtout en lumière que, comme dans le cas d'OpenSSL, des programmes Open

Source sont portés par une ou quelques personnes.

A lire aussi :

Le créateur de JavaScript lance son navigateur web, Brave
Le premier ransomware en JavaScript débusqué

crédit photo © ostill – shutterstock