GitHub va rendre obligatoire l'authentification double facteur

La filiale de Microsoft va exiger que tous les utilisateurs qui contribuent au code partagé sur la plateforme GitHub.com utilisent un mécanisme d'authentification double facteur (2FA).

Ils ont jusqu'à la fin d'année 2023 pour basculer massivement vers l'authentification multifacteur. « GitHub s'engage à ce que la sécurité forte des comptes ne limite pas une grande expérience développeur. Notre échéance – la fin 2023 – nous fournit l'opportunité d'optimiser cette démarche », déclare dans un billet de blog Mike Hanley, CSO de GitHub.

« À mesure que les normes évoluent, ajoute le directeur de la sécurité informatique (chief security officer), nous continuerons d'explorer activement de nouvelles façons d'authentifier en toute sécurité les utilisateurs, y compris via l'authentification sans mot de passe. »

Sécuriser la chaîne d'approvisionnement du logiciel

L'initiative vient compléter les actions déjà déployées pour renforcer la protection contre le piratage et la prise de contrôle de comptes de développeurs. La détection/invalidation de mots de passe utilisateur compromis, le support de WebAuthn ou encore la vérification de connexion (login) étendue à l'écosystème npm (Node Package Manager) en font partie.

L'action s'inscrit plus largement dans une démarche visant à sécuriser la chaîne d'approvisionnement des logiciels. Forte d'une communauté revendiquée de 83 millions de développeurs, l'entreprise ambitionne d'entraîner dans son sillage toute une industrie.

« La chaîne d'approvisionnement du logiciel commence avec les développeurs. Leurs comptes sont régulièrement ciblés par [des acteurs] de l'ingénierie sociale et du détournement de compte. La protection des développeurs contre ces types d'attaques est la première et la plus critique étape vers la sécurisation de la chaîne d'approvisionnement. » C'est en tout cas le message que veut faire passer le RSSI de la firme américaine.

Aussi, GitHub exhorte depuis des mois les développeurs à activer l'authentification multifacteur. L'été dernier, la société a abandonné l'authentification Git par mot de passe au profit de la 2FA. Elle pousse également l'authentification double facteur sur iOS et Android.

(crédit photo © GitHub)