GitHub abandonne les mots de passe au profit de la 2FA

Comme prévu, GitHub vient officiellement d'abandonner l'authentification Git par mot de passe. Une authentification plus forte est dorénavant requise pour toutes les opérations de gestion de version Git authentifiées sur GitHub.com, a expliqué la filiale de Microsoft.

Différentes options sont proposées. Les méthodes d'authentification multifacteur incluent les clés SSH ou les jetons d'accès personnels (tokens) pour les développeurs, les jetons d'installation OAuth ou GitHub App pour les intégrateurs, ou encore une clé de sécurité matérielle, telle que la clé YubiKey conçue par Yubico, partenaire de GitHub.

Il s'agit à la fois de protéger les utilisateurs et la plateforme de développement et de code partagé.

Authentification à double facteur

« Si vous ne l'avez pas déjà fait, veuillez prendre un moment pour activer l'authentification à double facteur (2FA) pour votre compte Github. Les avantages de l'authentification multifacteur sont largement documentés et protègent contre un large éventail d'attaques, dont le phishing », a souligné dans un billet de blog Mike Hanley, directeur de la sécurité informatique (CSO) de GitHub.

> *As of August 13, we no longer accept password authentication for Git operations. @_mph4 gives a rundown of available 2FA options – including a GitHub-branded YubiKey! https://t.co/wgQg9P0MZ0*
>
> *— GitHub (@github) August 16, 2021*

L'initiative vient s'ajouter aux mesures d'ores et déjà prises par GitHub pour renforcer la sécurité. « Nous avons beaucoup investi pour nous assurer que les communautés de développeurs de GitHub ont accès aux dernières technologies pour protéger leurs comptes contre les compromissions par des acteurs malveillants », a déclaré le RSSI. « Certains de ces investissements incluent des appareils vérifiés, le blocage de mots de passe compromis, le support de WebAuthn et la prise en charge des clés de sécurité pour les opérations SSH Git », a-t-il précisé.

(crédit photo @github)