Le 2FA de Github est idiot

SP SquonK (doc@sqk.fr)

30 novembre 2023

Résumé

Dans ce court article, je démontre que l'obligation de la part de Github d'activer le 2FA réduit la sécurité du système.

Introduction

Ce document, qui aurait dû être rédigé en anglais, est rédigé en français juste pour ajouter un peu de barrière de la langue aux décideurs.

Github est un des deux plus influents hébergeur de dépôts Git, l'autre étant Gitlab. Depuis très longtemps, Github imposait déjà le 2FA (2 Factor Authentification) : lorsque l'on se connecte depuis une nouvelle machine, le système nous envoie un code par email à saisir sur le site.

1 Les adresse email sont elles une mesure de 2FA ?

La réception d'un code par email constitue une forme de 2FA dans la mesure où pour se connecter, il faut le mot de passe et un accès à l'adresse email.

Il ne constitue pas une forme de 2FA dans la mesure où si on a uniquement l'accès à l'adresse email, on peut regénérer un mot de passe. Le mot de passe est donc parfaitement optionnel.

2 Les vraie mesures de 2Fa proposées par Github

Github propose plusieurs options pour le 2FA :

— Par SMS : cela nécessite de donner son numéro de téléphone à Github et de vivre avec son téléphone. Cette méthode est critiquée par les experts en sécurité car il est facile de compromettre des SMS. Cette méthode implique également de ne pas perdre son numéro de téléphone.

— Via une application mobile : cela nécessite également de vivre avec son téléphone, et donc de ne jamais le perdrE.

— En utilisant une clé USB de sécurité : vous perdez la clé, vous perdez l'accès à votre compte.

— Via un service de TOTP : Github vous donne un code, et pour vous connecter, vous devez calculer un code temporaire à partir du code et de l'heure actuelle. Souvent, le TOTP est résolu par téléphone (de base on vous présente un QR code qui contient le code initial) mais on peut également le stocker dans un gestionnaire de mot de passe ou faire son propre programme pour calculer le code temporaire.

3 A quel problème Github prétend répondre ?

Github prétend répondre au problème de la nécessité de sécuriser la chaîne de production des applications utilisant des solutions open source. Et Github ferait mieux de rester à sa place : la question du niveau de sécurisation des solutions open source devrait être défini non pas par Github, une entreprise commerciale, mais par les personnes qui maintiennent le projet en question, très souvent gratuitement.

"*Open source software is ubiquitous, with 90 percent of companies reporting that they use open source in their proprietary software. GitHub is a critical part of the open source ecosystem, which is why we take ensuring account security seriously.*" [1]

Si Github se met à se mêler de choses qui ne le regarde pas, aujourd'hui c'est le 2FA, demain c'est quoi ? Ils imposent de mettre à jour les logiciels qui sont hébergés par leur plate-forme quand des failles de sécurité sont découvertes ? C'est dans la même logique et pourtant on voit clairement que c'est pas leur rôle (ou alors, il faut qu'ils payent les personnes qui mettent leur code sur Github).

C'est aux personnes qui développent des logiciels propriétaires de s'assurer que les logiciels open source qu'ils utilisent sont conformes. C'est pas aux développeur open source de se plier aux désirs de personnes qui développent des logiciels propriétaires.

4 Imposer le 2FA réduit la sécurité des comptes

J'avais besoin de réacceder à mon compte Github pour désactiver un dépôt donc j'ai activé le 2FA par TOTP.

La première méthode qui rend le TOTP inefficace, c'est si le mot de passe du compte et le code TOTP sont stockés dans le même gestionnaire de mot de passe : dans ce cas, si l'un est compromis, l'autre l'est aussi.

Mais je n'utilise pas de gestionnaire de mot de passe. A la place, j'ai repris une application qui génère les code temporaires sur une page web, j'ai mis mes codes TOTP dessus et je l'ai mis sur le net. J'ai également mis mes codes à un autre endroit sur le net.

Pourquoi j'ai fait quelque chose d'aussi peu sûr ? Parce que mon activité sur Github ne demande pas à ce qu'il y ait un haut niveau de sécurité. Tous mes dépôts sont en public. Ceux qui ne le sont pas, au fond je m'en tape qu'ils soient un jour leaké. Le 2FA est pour moi un risque de perdre mon compte pour un gain totalement nul. Mon objectif est donc de minimiser ce risque.

Non seulement les mesures que j'ai prises ne sont pas sûres, mais par rapport à la politique précédente, l'obligation du 2FA augmente les risques pour rien : avant, lorsque je me connectais depuis une nouvelle localisation, je recevais un mail me demandant de valider la connexion. Maintenant je ne reçois plus de mail.

Enfin, l'obligation du 2FA est totalement hypocrite puisqu'elle ne s'applique que pour se connecter. On pouvait continuer à faire des commits et les pousser sur Github. **L'obligation de 2FA ne sécurise donc absolument pas les logiciels.**

Conclusion

Félicitations Github. Vous avez réduit la sécurité du compte d'au moins un utilisateur. Le 2FA ça marche que si la personne à qui vous l'imposez y voit un intérêt. Autrement dit, imposer le 2FA en dehors

1. https://github.blog/2023-03-09-raising-the-bar-for-software-security-github-2fa-begins-march-13/

de certains contextes très particulier (secteur bancaire, ...), ça ne marche pas.

Proposer le 2FA ? Expliquer son intérêt ? Permettre aux gestionnaire de projets de forcer les personnes qui ont des pouvoirs sur le projet ? Oui, très bonne idée. L'imposer pour tout le monde ? Non, restez à votre place.

Finissons donc cet article avec deux messages :

— Pour Github : Vous êtes très contents de faire des présentations sur " *The story of how we enforce 2FA for millions of users*" [2] mais les personnes impliquées dans l'obligation d'imposer le 2Fa devraient quitter leur travail et se tenir loin des emplois où elles peuvent nuire à l'humanité.

— Pour les accrocs au 2FA : Si l'idée de vivre dans un monde où il ne faut pas valider son identité sur une application 2FA avant de pouvoir respirer vous angoisse, consultez un spécialiste et laissez les autres bosser.

Et je ne vais pas non plus me fatiguer à relire.

Bibliographie

lol

2. https://github.com/orgs/community/discussions/74750