Communiqé de presse

Keeper® Security supporte désormais les clés de sécurité matérielles comme seule méthode 2FA

Les professionnels et les particuliers disposent désormais d'un contrôle encore plus grand sur l'utilisation des clés de sécurité pour une authentification pratique et hautement sécurisée.

PARIS, le 17 janvier 2024 – Keeper Security, le principal fournisseur de logiciels de cybersécurité Zero Trust et Zero Knowledge protégeant les mots de passe, les passkeys, les accès privilégiés, les secrets et les connexions à distance, présente aujourd'hui la prise en charge des clés de sécurité matérielles en tant que méthode unique d'authentification à deux facteurs (2FA). La mise en œuvre de l'authentification des utilisateurs à l'aide d'une seule clé de sécurité matérielle améliore la sécurité globale en fournissant un deuxième facteur physique solide, en atténuant les attaques à distance et en réduisant la dépendance à l'égard des appareils mobiles. Les administrateurs peuvent imposer l'utilisation d'une clé matérielle comme seule méthode d'authentification à deux facteurs et imposer des restrictions encore plus strictes en exigeant l'utilisation d'un code PIN.

Les facteurs d'authentification renforcés deviennent de plus en plus importants à mesure que les cybercriminels deviennent plus sophistiqués, brisant ce qui était auparavant considéré comme des défenses à toute épreuve. Les méthodes traditionnelles d'authentification 2FA, telles que le SMS et le TOTP (Time-Based One-Time Password), peuvent être vulnérables à l'ingénierie sociale et à l'échange de cartes SIM. En fait, le National Institute of Standards and Technology (NIST) a retiré l'utilisation de l'authentification par SMS de sa liste de méthodes d'authentification recommandées en raison de ses vulnérabilités. Cette situation a conduit les organisations et les particuliers à rechercher des alternatives plus sûres à l'authentification par mot de passe électronique.

« Les cybercriminels sont créatifs et implacables dans leur mission de briser les solutions historiquement sécurisées », a déclaré Craig Lurey, CTO et cofondateur de Keeper Security. « En réponse, de nombreuses organisations passent à des dispositifs 2FA matériels tels que YubiKey. Avec Keeper, les administrateurs peuvent désormais imposer l'utilisation d'une clé de sécurité matérielle comme seule option 2FA, donnant aux utilisateurs une méthode d'authentification simple et conviviale, mais hautement sécurisée. »

Bien que la prise en charge des clés de sécurité matérielles ne soit pas une nouveauté pour Keeper®, les utilisateurs devaient auparavant disposer d'une option 2FA de secours en plus de leur clé de sécurité. Désormais, les entreprises et les particuliers peuvent avoir une clé de sécurité comme seule méthode 2FA. Keeper permet aux utilisateurs d'avoir plusieurs clés de

sécurité, permettant aux utilisateurs d'avoir des clés de sauvegarde, des clés dans plusieurs endroits ou des clés pour plusieurs appareils.

Les utilisateurs existants peuvent se connecter à Keeper Web Vault ou Keeper Desktop App version 16.10.12+ pour supprimer les autres méthodes de 2FA s'ils préfèrent n'utiliser qu'une clé de sécurité seule. Les administrateurs peuvent également demander à leurs utilisateurs d'activer un PIN (vérification de l'utilisateur FIDO2) avec leur clé de sécurité, protégeant ainsi davantage leurs organisations. Keeper supporte la connexion sur les appareils iOS et Android avec une clé de sécurité. Cependant, la configuration d'une clé de sécurité comme seule méthode 2FA doit être effectuée sur le Web Vault ou Keeper Desktop App.

Il s'agit de la dernière amélioration apportée aux solutions de Keeper, après l'annonce de Granular Sharing Enforcements pour sa plateforme. Les entreprises choisissent Keeper en raison de sa solide architecture de sécurité, de sa capacité à prendre en charge l'authentification fédérée et sans mot de passe avec n'importe quel fournisseur d'identité, de son intégration transparente dans les environnements sur site, cloud ou hybrides, et de sa facilité d'utilisation sur les ordinateurs de bureau et les appareils mobiles. Keeper Security Government Cloud Password Manager et Privileged Access Manager est autorisé par FedRAMP et StateRAMP, et maintient le cadre de sécurité Zero Trust et Zero Knowledge de Keeper Security aux côtés d'une architecture de sécurité Zero Trust et Zero Knowledge, de sorte que les utilisateurs ont une connaissance, une gestion et un contrôle complets de leurs informations d'identification et de leurs clés de chiffrement.

###

A propos de Keeper Security:
Keeper Security transforme la cybersécurité pour les personnes et les organisations du monde entier. Les solutions de Keeper, abordables et faciles à utiliser, sont construites sur la base d'une sécurité Zero Trust et Zero Knowledge pour protéger chaque utilisateur sur chaque appareil. La solution de gestion des accès privilégiés de nouvelle génération Keeper se déploie en quelques minutes et s'intègre de manière transparente à n'importe quelle stack technologique pour prévenir les violations, réduire les coûts du service d'assistance et garantir la conformité.Des millions de personnes et des milliers d'organisations font confiance à Keeper, le leader en matière de gestion de mots de passe et de passkeys, de gestion des secrets, d'accès privilégié, d'accès à distance sécurisé et de messagerie chiffrée.

Pour en savoir plus, visitez le site KeeperSecurity.com
Suivre Keeper: Facebook Instagram LinkedIn X YouTube

Contact Presse :