LastPass affecté par une faille critique d’accès à distance

LastPass affecté par une faille critique d’accès à distance

Le chercheur en sécurité Tavis Ormandy a repéré une faille critique dans LastPass qui permettrait d'établir un accès à distance dans le gestionnaire de mots de passe. Un signalement à LastPass a été effectué, qui prépare un correctif.

Les gestionnaires de mots de passe peuvent se montrer d'une grande aide pour celui qui tient à conserver en un seul endroit une multitude de codes d'accès. Surtout, ils satisfont d'un coup plusieurs exigences en matière de sécurité informatique qui sont parfois contradictoires ou inapplicables au-delà d'un certain seuil.
Regardons un instant ce que l'on demande en règle générale à l'usager : l'utilisation d'un mot de passe unique par service, tout en respectant un strict formalisme qui va de la longueur du mot de passe (x caractères au minimum) à sa complexité (des lettres, des chiffres, des symboles, des majuscules et des minuscules, en mélangeant le tout), en passant par son renouvellement (sait-on jamais).

Bien entendu, il est évidemment tout à fait déconseillé de les noter simplement sur un bout de papier (on n'est jamais trahi que par les siens) ou de les enregistrer dans un fichier sur le PC (qui peut se faire pirater). Or, la seule mémorisation n'est pas une solution d'avenir : au-delà de quelques services, l'utilisateur s'y perdrait. D'où l'intérêt de passer par des gestionnaires de mots de passe.

Mais leur utilité ne doit pas faire oublier le fait que ces programmes sont par essence imparfaits.
Malgré tout le soin qui peut être apporté pendant leur conception, ces logiciels (les plus connus sont Dashlane, 1Password, KeePass et LastPass) peuvent être sensibles à certaines attaques. On l'a vu par exemple avec LastPass, qui est annoncé comme vulnérable au hameçonnage et qui a essuyé une intrusion dans son infrastructure, a priori sans dommage pour les mots de passe eux-mêmes.
Dans ce contexte, des initiatives comme celle lancée par la Commission européenne, qui consiste à organiser un audit du code source de KeePass – qui est un logiciel libre, ce qui facilite grandement les choses – sont à accueillir avec bienveillance. Elles contribuent à un rehaussement général du niveau de fiabilité de ce type de logiciel, à défaut de le rendre invulnérable, ce qui est illusoire.
La contribution d'un chercheur comme Tavis Ormandy est aussi précieuse, même si de prime abord elle provoque légitimement une inquiétude sur le degré de finition de certains logiciels. En effet, l'intéressé indique avoir déniché dès le premier coup d'œil une série de problèmes critiques qui lui ont sauté aux yeux. Il a ajouté avoir fait suivre un rapport complet à LastPass pour qu'il les règle.
La nature des vulnérabilités repérées n'est pas précisée par Tavis Ormandy. Le blog Naked Security, édité par l'éditeur d'antivirus Sophos, écarte pour le moment la piste de la faille 0-Day. Une telle vulnérabilité désigne les brèches n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. Elles sont les plus dangereuses, car elles sont secrètes et peuvent être exploitées en toute discrétion.
Tout juste sait-on que la vulnérabilité en question permettrait un accès complet à distance. L'on peut imaginer que des détails supplémentaires seront donnés ultérieurement, lorsque LastPass aura fini son intervention. Dans un autre tweet, Tavis Ormandy ajoute qu'il va se pencher dans la foulée sur 1Password et regarder s'il peut repérer des fragilités dans ce gestionnaire.
Dans le cadre d'une divulgation responsable, les spécialistes en sécurité informatique sont en effet invités à signaler d'abord aux sociétés les failles qu'ils repèrent dans les logiciels qu'elles éditent, et cela en toute discrétion. Ce n'est qu'ensuite qu'une diffusion publique peut avoir lieu, une fois les correctifs appliqués, de façon à ce que des personnes mal intentionnées ne puissent pas en profiter.
Tavis Ormandy est une pointure dans le domaine de la sécurité informatique.
Il s'est illustré à diverses reprises en signalant des brèches critiques dans un certain nombre de logiciels, comme Linux, Windows, la plateforme de jeux Uplay conçue par Ubisoft ou encore le shell Bash. Il a aussi épinglé les éditeurs d'antivirus Sophos et Trend Micro. Il travaille depuis quelques années dans l'équipe Project Zero mise sur pied par Google pour traquer les failles 0-Day, qui regroupe quelques personnalités. À tel point qu'elle est présentée comme une dream team.
Article original de Julien Lausson

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : LastPass affecté par une faille critique d’accès à distance – Tech – Numerama