# Clickjacking et gestionnaires de mots de passe

Depuis août 2025, plusieurs publications techniques (IT-Connect, The Hacker News) signalent une vulnérabilité critique baptisée « DOM-based extension clickjacking » affectant les extensions des principaux gestionnaires de mots de passe (1Password, LastPass, Bitwarden, etc.). Le DOM, Document Object Model, représente la structure HTML d'une page web et permet aux scripts et aux extensions d'interagir avec les éléments de la page. L'attaque exploite cette structure en superposant des éléments invisibles sur des boutons légitimes : lorsqu'un utilisateur clique, l'extension déclenche en arrière-plan l'autoremplissage et envoie sans le vouloir les identifiants, codes TOTP ou passkeys au serveur de l'attaquant. Les tests présentés à DEF CON 33 ont montré que 10 extensions sur 11 étaient vulnérables et 9 exposaient les secrets d'authentification à deux facteurs, ce qui représente des millions d'installations actives.

Dans une entreprise, ce type d'attaque est critique. Les gestionnaires de mots de passe y stockent souvent les comptes administrateurs AD, les accès VPN, les identifiants de serveurs ou d'applications internes. Le problème est d'autant plus sensible que l'attaque ne nécessite pas de faille complexe côté poste client : un seul clic sur une page piégée suffit.

Pour réduire le risque, il est recommandé de pousser immédiatement les mises à jour correctives des extensions, de désactiver ou restreindre l'autofill, d'activer le verrouillage automatique des coffres et de configurer une correspondance stricte des domaines pour l'autoremplissage. Cette vulnérabilité rappelle qu'un outil de sécurité peut devenir un vecteur d'attaque s'il n'est pas maintenu et configuré correctement.

https://www.it-connect.fr/le-clickjacking-menace-les-donnees-des-gestionnaires-de-mots-de-passe-les-plus-populaires/

https://thehackernews.com/2025/08/dom-based-extension-clickjacking.html