Vulnerabilități zero-day de tip clickjacking în gestionarele de parole

Introducere	În luna august 2025, cercetătorul în securitate *Marek Tóth* a prezentat la *DEF CON 33* o nouă tehnică de clickjacking aplicată extensiilor de navigator, denumită „*DOM-based Extension Clickjacking*”. Spre deosebire de *clickjacking*-ul clasic în care utilizatorul este păcălit să facă clic pe un element ascuns într-un iframe, tehnica lui Tóth manipulează elementele interfeței de utilizator injectate de extensii direct în *Document Object Model* (DOM) al paginii. Prin ajustarea opacității și suprapunerea acestor elemente, scripturile rău intenționate le fac invizibile dar clicabile, iar un singur clic pe bannere aparent legitime (de exemplu, ferestre de consimțământ pentru cookie-uri sau *CAPTCHA*) poate declanșa autofurnizarea datelor sensibile stocate în managerul de parole.
Conceptul de clickjacking	*Clickjacking* (sau redresarea interfeței) este un atac de tip client-side în care straturile vizuale sunt manipulate pentru a deturna clicurile utilizatorului. În varianta clasică, atacatorul încarcă site-ul vizat într-un *iframe* invizibil și plasează deasupra un element vizibil. Clicurile utilizatorului sunt interceptate de *iframe*, permițând efectuarea de acțiuni malițioase pe site-ul țintă. Măsurile tradiționale precum antetele ***X-Frame-Options*** sau politicile ***Content-Security-Policy*** reduc eficacitatea *clickjacking*-ului web.
Evoluția către extensii de browser	Gestionarele de parole s-au mutat în mare parte în extensii de navigator. Aceste extensii injectează elemente *UI* (de exemplu, butoane pentru completare automată) direct în *DOM*, iar atacatorii pot aplica stiluri *CSS* (de exemplu, ***opacity: 0***) pentru a le face invizibile și suprapuse peste elemente aparent inofensive. Când utilizatorul încearcă să interacționeze cu un banner de cookie sau o verificare *CAPTCHA*, clicul activează de fapt butonul invizibil al extensiei și declanșează completarea automată a formularelor cu datele sale.
Metodologia de testare	Managerii de parole sunt utilizați pe scară largă ca extensii de browser pentru a simplifica autentificarea pe site-uri web. În cadrul acestui studiu, au fost testați 11 manageri de parole folosind o tehnică nouă. Pentru selecția a 10 manageri, a fost folosit articolul PCMag „Cei mai buni manageri de parole pentru 2025”. Managerii enumerați acolo sunt: ✓ 1Password ✓ Bitwarden ✓ Dashlane ✓ Enpass ✓ Keeper ✓ LastPass ✓ LogMeOnce ✓ NordPass ✓ ProtonPass ✓ RoboForm La această listă a fost adăugat și iCloud Passwords, datorită utilizării pe scară largă (5,4 milioane de instalări active — Chrome Web Store, Firefox Add-ons, Edge Add-ons).

<table>
<tr><td></td><td>Se menționează că iCloud Passwords a fost testat doar ca extensie de browser (Google Chrome, Firefox etc.), nu ca aplicație de sistem cu integrare Safari.</td></tr>
<tr><td>Rata de vulnerabilitate</td><td>Rezultatele au fost alarmante: toate cele 11 extensii testate au fost vulnerabile cel puțin la o variantă a tehnicii DOM-based Extension Clickjacking. Estimările cercetătorului indică aproximativ 40 milioane de instalări active afectate în total pe platformele Chrome Web Store, Firefox Add-ons și Edge Add-ons.

Cercetarea a împărțit impactul în trei categorii:
✓ Extragerea detaliilor cardului de credit – șase din nouă manageri testați cu funcție de card au permis scurgerea codurilor de securitate și a numerelor cardului.
✓ Exfiltrarea informațiilor personale – opt din zece manageri au fost vulnerabili la accesarea datelor precum nume, adresă sau număr de telefon.
✓ Furtul de credențiale și coduri TOTP – zece din unsprezece manageri au permis extragerea credențialelor de logare, inclusiv coduri TOTP folosite la autentificarea în doi pași</td></tr>
<tr><td>Manager de parole vulnerabile vs. remediați</td><td>După dezvăluirea responsabilă din aprilie 2025, unele companii au lansat remedii. Conform articolului Cyber Security News, următorii manageri au remediat vulnerabilitatea până în august 2025: Dashlane, Keeper, NordPass, ProtonPass și RoboForm.
Celelalte – 1Password, Bitwarden, LastPass, iCloud Passwords, Enpass și LogMeOnce – rămân vulnerabile, reprezentând aproximativ 32,7 milioane de instalări active încă expuse.</td></tr>
<tr><td>Statusul remedierii</td><td>
<table>
<tr><th>Manager de parole</th><th>Manager de parole</th><th>Manager de parole</th></tr>
<tr><td>1Password</td><td>Vulnerabil</td><td>Raportul sugerează că furnizorul a marcat vulnerabilitatea ca „informativă” și nu a planificat o remediere rapidă.</td></tr>
<tr><td>Bitwarden</td><td>Vulnerabil</td><td>Se lucrează la corectare, dar încă nepublicată.</td></tr>
<tr><td>LastPass</td><td>Vulnerabil</td><td>Răspuns lent; considera problema în afara programului de recompense.</td></tr>
<tr><td>iCloud Passwords</td><td>Vulnerabil</td><td>Versiunea 3.1.25 este încă afectată.</td></tr>
<tr><td>Enpass</td><td>Vulnerabil</td><td>În dezvoltare remedierea.</td></tr>
<tr><td>LogMeOnce</td><td>Vulnerabil</td><td>Nu a răspuns la raportare; nicio actualizare.</td></tr>
<tr><td>Dashlane</td><td>Remediat</td><td>A lansat patch-uri după dezvăluire.</td></tr>
<tr><td>Keeper</td><td>Remediat</td><td>Remediat prin actualizări.</td></tr>
<tr><td>NordPass</td><td>Remediat</td><td>A aplicat corecturi.</td></tr>
<tr><td>ProtonPass</td><td>Remediat</td><td>A lansat versiuni corectate.</td></tr>
<tr><td>RoboForm</td><td>Remediat</td><td>Corecțiile sunt disponibile.</td></tr>
</table>
</td></tr>
<tr><td colspan="2">Scenarii de atac și impact asupra utilizatorilor</td></tr>
<tr><td>Site controlat de atacator</td><td>În primul scenariu, atacatorul creează un site ce conține scripturi malițioase. Acestea fac invizibile elementele UI ale extensiei de manager de parole (prin</td></tr>
</table>

	opacity și suprapuneri) și le așază sub bannere convingătoare (de ex. consimțământ cookie, ferestre de abonare). Utilizatorul este îndemnat să facă clic pentru a închide bannerul, dar clicul activează de fapt funcția de autofurnizare a managerului de parole, iar datele (carduri, adrese, credențiale) sunt trimise automat. Pe această cale, atacatorul poate fura informațiile fără a exista vulnerabilități pe site-urile legitime.
Vector de atac prin subdomeniu	O vulnerabilitate și mai gravă rezultă din modul în care managerii de parole completează credențialele pe toate subdomeniile domeniului inițial. Cercetarea arată că atacatorii pot exploata vulnerabilități de tip ***cross***-site scripting (XSS) sau pot prelua controlul asupra unui subdomeniu pentru a injecta scriptul de *clickjacking*. Deoarece managerii completează automat informațiile pe orice subdomeniu, un atacator care găsește o vulnerabilitate ***XSS*** pe un subdomeniu poate fura credențialele contului principal și codurile ***TOTP***
Măsuri de protecție și recomandări	
Pentru utilizatori	✓ Schimbați modul de acces al extensiei în „la clic”. Pe browserele bazate pe Chromium, configurați accesul extensiei doar la cerere, pentru a controla manual când se completează datele. ✓ Actualizați extensiile managerului de parole. Unele companii au publicat patch-uri; verificați că folosiți versiunea cea mai recentă și parcurgeți nota de securitate. ✓ Dezactivați funcția de completare automată. Dacă există opțiune de completare manuală, activați-o; necesită un pas suplimentar dar reduce expunerea. ✓ Fiți precauți cu site-urile necunoscute. Nu faceți clic pe bannere suspecte și utilizați instrumente de securitate (script-blockers, filtre anti-tracking) pentru a limita posibilitatea injectării de scripturi malițioase.
Pentru dezvoltatorii de gestionare de parole	✓ Implementați verificări de interfață la nivel de extensie. Adăugați logică ce detectează când elementele UI sunt invizibile sau suprapuse, pentru a preveni utilizarea lor într-un context nefiresc. ✓ Restricționați resursele accesibile. Folosiți parametri ***matches*** în manifestul extensiei (web_accessible_resources) pentru a limita încărcarea resurselor ***HTML/JS*** doar de pe domenii de încredere ✓ Aplicați antete de securitate. Răspunsurile servite prin web_accessible_resources trebuie să includă antete ***X-Frame-Options: DENY*** sau ***Content-Security-Policy***: frame-ancestors 'none' pentru a împiedica încărcarea în iframe-uri invizibile. ✓ Oferiți control granular asupra autofurnizării. Permiteți utilizatorilor să aleagă modul de completare (manual/automat) și restricționați completarea la domeniul exact corespunzător. ✓ Răspundeți prompt la rapoartele de vulnerabilitate. Ignorarea sau marcarea lor ca „informative” lasă utilizatorii expuși, iar reacțiile întârziate afectează încrederea.
Referință	https://marektoth.com/blog/dom-based-extension-clickjacking/#:~:text=The%20following%20password%20managers%20were,listed%20there https://cybersecuritynews.com/0-day-clickjacking-vulnerabilities/