CVE-2025-4096

Scor	8.8 (RIDICAT)
CWE	**CWE-122**: Scriere în afara limitelor heap-ului (Heap-Based Buffer Overflow)
Descrierea	CVE-2025-4096 este o vulnerabilitate critică de tip heap buffer overflow identificată în motorul de procesare *HTML* al browserelor *Chromium*, inclusiv *Google Chrome*. Aceasta permite unui atacator să trimită conținut *HTML* malițios pentru a declanșa o corupere a memoriei, cu posibilitatea de a executa cod arbitrar, de a provoca prăbușirea aplicației sau de a accesa date sensibile. Vulnerabilitatea necesită interacțiunea utilizatorului, cum ar fi accesarea unei pagini web special concepute.
Versiunea afectată	Anterioare versiunii 136.0.x
Componentă	Motorul de randare *HTML*
Metoda de exploatare	1. Pregătirea unui payload *HTML* malițios: • Atacatorul creează o pagină web care conține un set de elemente *HTML* nestandard (ex: ***<template>, <iframe>, <object>,*** manipulări ale *DOM* shadow sau pseudo-elemente CSS) ce induc comportament neașteptat în parserul *HTML*. • Se abuzează de o funcție care realizează o operațiune de copiere (ex: ***memcpy***, ***memmove***, ***CopyCharacters***) fără o verificare corespunzătoare a dimensiunii bufferului alocat. 2. Declanșarea erorii în momentul renderizării: • Browserul, în timpul construirii arborelui *DOM* sau al layout-ului *CSS*, ajunge să scrie dincolo de limita bufferului alocat în heap. • În funcție de structura memoriei și protecțiile active (ex: ASLR, DEP), acest overflow poate: ✓ Corupe date din alte obiecte *HTML*. ✓ Suprascrie pointeri de funcție sau vtab-uri virtuale (în *C++*). ✓ Crea condiții pentru execuție de cod arbitrar (*RCE*). 3. Escaladarea efectelor exploatării: • Dacă browserul rulează fără sandboxing corespunzător sau dacă atacatorul combină vulnerabilitatea cu un alt exploit (ex: un sandbox escape, CVE chaining), poate obține acces la sistemul de operare sau poate fura date sensibile (ex: cookie-uri, tokenuri, date din memorie). 4. Persistență și exfiltrare: • Exploitul poate fi folosit pentru a injecta cod *JavaScript* persistent sau pentru a deschide canale de comunicare către servere *C2* (Command and Control), exfiltrând datele browserului.
Metoda de detectare	• Monitorizare comportament browser – urmărirea crash-urilor neobișnuite sau accesări suspecte de memorie. • Scanare cu instrumente de analiză statică – analiza surselor *HTML* și JavaScript injectate. • Instrumente *EDR/AV* – detecție de exploituri de tip heap overflow.

CVE-uri asociate	• CVE-2023-2033 – similar, heap buffer overflow în V8 (motor JavaScript) • CVE-2024-0519 – exploatare remote în componenta WebAssembly • CVE-2024-2883 – ocolire a sandboxului în Chromiu
Recomandări	• Actualizați Google Chrome la versiunea 136 sau una ulterioară care conține patch-ul oficial. • Activați actualizările automate în browser pentru a beneficia de patch-uri viitoare de securitate. • Evitați accesarea site-urilor necunoscute sau suspecte. • Activarea protecțiilor de memorie precum ASLR, DEP/NX, Stack Canaries. • Folosirea containerizării aplicațiilor (Chrome rulează deja fiecare tab în sandbox separat). • https://www.tenable.com/cve/CVE-2025-4096?utm_source=chatgpt.com • https://securityonline.info/chrome-update-fixes-high-severity-security-flaw-cve-2025-4096/ • https://gbhackers.com/chrome-136-fixes-20-year-old-privacy-bug/?utm_source=chatgpt.com