

Darius — Independent Security Scan (full report)

Generated by extensionsecurity.io, a free third-party scanner not affiliated with or controlled by Darius. Full, unedited results below — including the two items it flagged, with a plain-language explanation of what they actually are.

extensionsecurity.io

The Only Multi-Browser Extension Security Scanner

Assess the security and privacy risks of browser extensions across Chrome, Edge, and Firefox, for free. No sign up required.



Start a new scan

Darius — Memecoin Risk Scanner

Automatically scans memecoins for scam risks (rug pulls, honeypots) on DexScreener, Pump.fun, Birdeye and more.

[View extension code](#)

Version

1.2.0

Navigator

Chrome

Risk profile

A+

Risk Score: 13

Privacy policy

Not found

Website

Not found

Contact

Not found

Security risk score per category (The higher the score, the higher the risk)

Permissions	Cross-origin policies	Tracking & Privacy	Obfuscation	Vulnerabilities	Domains & URLs
10	50	6	0	0	0

Permissions

Cross-origin policies

Tracking

Obfuscation

Vulnerabilities

Domains & URLs

Risks summary

Permissions

Risk score: 10

Low risk permissions

storage

Allows storing data locally.

low

alarms

Allows scheduling tasks to execute at specific times.

low

Overall: A+ rating, risk score 13/100 (lower is safer). Only two permissions detected (storage, alarms), both rated "low risk" by the scanner itself.

Vulnerabilities — score 0

Vulnerabilities

Risk score: 0

Vulnerable libraries count
0

Impacted files count
0

Per severity level

critical
0

high
0

medium
0

low
0



No vulnerabilities detected
No known vulnerabilities have been found in any javascript libraries used by this extension.

No known vulnerabilities in any JavaScript library Darius uses.

Domains & URLs — no malicious domains detected

Domains & URLs

Risk score: 0

Malicious domains



No known malicious domains detected.

The extension may communicate with the following domains and URLs:

www.helius.dev US
76.76.21.21 United States, Walnut
URLs found:
<https://www.helius.dev/>

public-api.birdeye.so US
172.66.161.182 United States
URLs found:
https://public-api.birdeye.so/defi/token_securit...

token.jup.ag
Unknown IP
URLs found:
<https://token.jup.ag/strict>

api.basescan.org US
184.26.12.113 United States
URLs found:
<https://api.basescan.org/api>

api.etherscan.io US
217.79.243.34 United States, Tampa
URLs found:
<https://api.etherscan.io/api>

api.bscscan.com US
91.191.210.250 United States, Tampa
URLs found:
<https://api.bscscan.com/api>

docs.birdeye.so US

reactis.org US

api.mainnet-beta.solana.com US

Every domain Darius contacts is a well-known public blockchain data provider (Helius, Birdeye, Jupiter, BaseScan, Etherscan, BscScan, Solana RPC, etc.) — the same public APIs anyone could query manually from a browser or terminal.

Risk summary

Risk summary



No risky permission combinations detected

This extension does not use known permission combinations that pose a risk to your security and privacy.

Cross-origin policies — score 50

Cross-origin policies

Risk score: **50**

Content Security Policy (CSP)

low

A Content Security Policy (CSP) for an extension helps protect users by defining which sources of content are allowed to be executed within a web page, thereby preventing cross-site scripting (XSS) attacks and other malicious scripts. By specifying allowed sources, CSP ensures that only trusted content is loaded, enhancing the security of the extension and the websites it interacts with.

Value:

Not defined

No CSP policy defined, therefore the default policy applies : **script-src 'self'; object-src 'self'**

Cross Origin Embedder Policy (COEP)

high

The Cross-Origin Embedder Policy (COEP) for an extension controls the loading of cross-origin resources, requiring them to have appropriate CORS or CORP headers to be embedded, thus enhancing security by preventing unauthorized resource loading. By setting COEP, an extension can opt into cross-origin isolation, enabling the use of powerful features like SharedArrayBuffer while ensuring secure resource embedding.

Value:

Not defined

No COEP policy defined, therefore the default unsafe policy applies : **unsafe-none**

Cross Origin Opener Policy (COOP)

high

The Cross-Origin Opener Policy (COOP) for an extension helps isolate its browsing context, preventing cross-origin interactions that could lead to data leaks or security vulnerabilities. By specifying a COOP value, an extension can control whether new windows or tabs it opens are isolated from its own context, enhancing security against potential attacks like XS-Leaks.

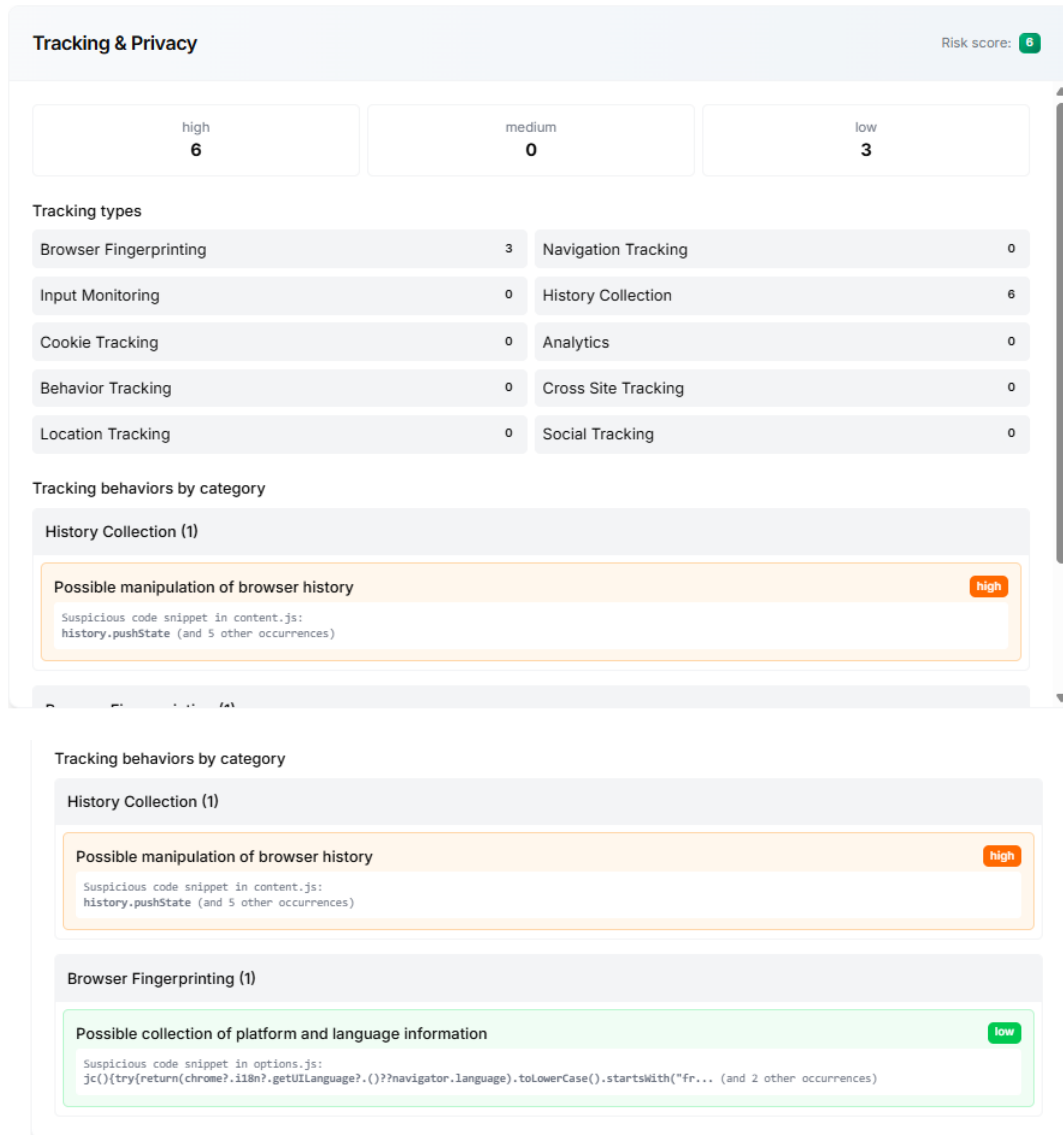
Value:

Not defined

No COOP policy defined, therefore the default unsafe policy applies : **unsafe-none**

What this actually means: CSP, COEP and COOP are optional web-security headers, most relevant to full web pages that need to isolate themselves for advanced browser features (like SharedArrayBuffer). Darius doesn't use any such feature, so it doesn't set them — this is the default, standard state for the large majority of Chrome extensions, not a sign of anything being exploited. Chrome's own built-in extension sandboxing applies regardless.

Tracking & Privacy — score 6



"Possible manipulation of browser history" (flagged high) — what it actually is: Darius runs on trading platforms (Axiom, Pump.fun, BullX...) that are single-page apps: they change the token you're viewing without reloading the page. The only way to detect that a new token was opened is to watch for URL changes via `history.pushState`. Darius reads this event to know when to re-scan — it never rewrites, deletes, or redirects your browser history. The scanner flags the pattern because it *could* be used maliciously elsewhere; here it's used exactly once, for page-change detection.

"Possible collection of platform and language information" (flagged low) — what it actually is: This is Darius checking `navigator.language` once, to decide whether to show its interface in French or English. Nothing is sent anywhere — it only changes which language is displayed locally, in your own browser.

You can re-run this scan yourself at any time at extensionsecurity.io — no sign-up required.