Perplexity Comet Browser Vulnerable To Prompt Injection Exploit via @sejournal, @martinibuster



Brave published details about a security issue with Comet, Perplexity's AI browser, that enables an attacker to inject a prompt into the browser and gain access to data in other open browser tabs.

Comet AI Browser Vulnerability

Brave described a vulnerability that can be activated when a user asks the Comet AI browser to summarize a web page. The LLM will read the web page, including any embedded prompts that command the LLM to take action on any open tabs

According to Brave:

> *"The vulnerability we're discussing in this post lies in how Comet processes webpage content: when users ask it to*

> *“Summarize this webpage,” Comet feeds a part of the webpage directly to its LLM without distinguishing between the user’s instructions and untrusted content from the webpage. This allows attackers to embed indirect prompt injection payloads that the AI will execute as commands. For instance, an attacker could gain access to a user’s emails from a prepared piece of text in a page in another tab.”*

A post on Simon Willison’s Weblog shared that Perplexity tried to patch the vulnerability but the fix does not work.

A developer posted the following on X:

> *“Why is no one talking about this?*
>
> *This is why I don’t use an AI browser*
>
> *You can literally get prompt injected and your bank account drained by doomscrolling on reddit:”*

Things aren’t looking good for Comet Browser at this time.

https://www.searchenginejournal.com/perplexity-comet-browser-vulnerable-to-prompt-injection-exploit/554575/