CXOtoday.com
IT Perspective for Decision Makers

The hidden cyber threat in agentic AI browsers

Agentic browsers are a security risk as they can act autonomously and access sensitive data, creating new attack surfaces.

Last month, security researchers at Brave web browser found that Perplexity's Comet's AI assistant was unable to distinguish between user commands and malicious instructions hidden in web pages, making it susceptible to executing malicious commands.

Researchers warn that these AI assistants and agents operate with a user's full privileges across authenticated sessions, which gives them access to user's bank accounts, emails, cloud storage, and other sensitive data, thus increasing the risk of breaches.

The reason: Generative AI (GenAI)-powered chatbots that can retrieve real-time information within seconds have become the go-to search medium for millions. They are now part of most leading web browsers, which are now planning to supplement them with agentic AI tools that can summarize web pages, fill forms, and book flights or hotel rooms on behalf of users.

The global AI browser market is expected to grow to $76.8 billion in 2034 from $4.5 billion in 2024, according to a Market.us report. Though Google Chrome remains the most popular web browser with 69% market share as per Statcounter, it faces challenges from Comet and OpenAI's upcoming AI browser.

But the convenience of getting quick and crisp responses or delegating tasks to an agent, comes with its share of new risks stemming from GenAI and agentic AI's access to sensitive user data and the autonomy to act on their own. When used in a work environment, these AI-powered web browsers can put enterprises and their data at risk.

Nikesh Arora, CEO of Palo Alto Networks, echoed these concerns last month at his company's Q4 FY25 earnings call, when he warned that all leading web browsers are soon going to get agentic AI tools that will seek access to users' browsers to perform tasks such as booking a hotel room or a table at a restaurant. This can be a concern for enterprises as they don't want employees on browsers that can run AI agents without control.

Until now web browsers have been used to search and view content. With agentic AI, they will get the ability to interact with user data, applications, and network resources.
Why agentic AI browsers pose a threat?
While many organizations use network monitoring tools to keep track of all web browsing activities of employees, browsers with agentic AI come with certain security risks such as prompt injection attacks. They can also mimic humans making it difficult for security tools to flag malicious scripts or bot traffic.

"Agentic AI tools are essentially automation scripts that perform routine cognitive tasks at scale, reducing costs and human effort. While powerful, they come with inherent risks. Lacking situational awareness, they can miss nuances and fail to prioritize the most urgent threats, leaving organizations exposed," said Sanjay Katkar, Joint Managing Director, Quick Heal Technologies.

Katkar added that they are also vulnerable to targeted manipulation, where poisoning attacks can trick them into stealing sensitive information.

Aaron Bugal, Field Chief Information Security Officer for APJ at Sophos, points out that "organisations need to be, bare minimum, aware of where these applications may exist within their fleet of user devices."

According to Bugal, anything that happens within the browser is potentially able to be transported to where the agentic AI requests are processed.

"It can include searches, posted information and potentially objects within the browser that would otherwise be under the control of the user, but in this case 'shared' with the browser provider – cookies and security tokens to name a few – let alone the information the browser has been granted access to," he added.

Unlike traditional vulnerabilities in web browsers that target individual websites and use complex exploitation tactics, prompt injection attacks are much easier to carry out using natural language instructions, researchers warned.

Further, a study by University of California, Davis, released last month, shows that GenAI browser assistants collect "personal and sensitive information" and share it with first-party servers as well as third-party trackers such as Google Analytics.

What can enterprises do about them

Experts believe that AI governance policies with guidelines on which applications can and cannot be installed and use of controls to ensure employees can't violate them can be effective in mitigating the threat of agentic browsers.

Security researchers at Brave browser opine that agentic capabilities should be isolated from regular browsing tasks, so a user can't accidentally end up on this mode while browsing. "This clean separation is especially important in these early days of agentic security, as browser vendors are still working out how to prevent security and privacy attacks," they added.

Enterprises on their part need to weigh up if and when these types of browsers are suitable for use internally and conduct a risk assessment, cautions Bugal, adding, "regardless, policies and technical controls should be considered and applied to this and other technologies available to the user."

Bugal further said that it’s important that organisations evaluate how they can monitor and regulate access to the internet by employees from their work devices. “Having the ability to detect and respond to misuse of corporate assets and the information that has access to is something every business needs to have,” he added.

Palo Alto’s Arora believes that one way to counter potential threats originating from agentic browsers is to deploy defensive AI agents that can also act on their own. ManyAI browsers are still in early stages of adoption, hence enterprises will do well to heed such advice.