**An unpatched Safari issue can expose browser history and other personally identifiable information.**

Apple is aware of the issue and is working to resolve it.



**What's at stake:** Safari 15 has a problem that allows a website to access your recent browser history, as well as your Google account ID and avatar, according to researchers. Since Sunday, January 16, Apple has been aware of the issue and has been working on a patch. As of January 18, no patch had been issued by the developers.

The flaw is said to be connected to the IndexedDB API, according to security firm FingerprintJS. A page from one domain's database cannot be viewed by another website in most browsers. The API's implementation in Safari, on the other hand, breaches the "same-origin policy," giving a rogue website enough information to identify Safari users.

In a video broadcast on January 14, FingerprintJS describes its proof-of-concept (POC) demo (below). It also made a live copy of the POC available on the web for anyone interested in seeing it in action.

On November 28, the researchers submitted the vulnerability (233548) to the WebKit Bug Tracker for the first time. Apple employees tagged the bug report as addressed as of this weekend, however sources at TechSpot can confirm that the current version of Safari is still unfixed as of January 18.

Bad actors might use this issue to identify users via a lookup table, according to FingerprintJS. Authenticated databases can also expose a user's unique ID and profile picture, allowing the person to be identified even more precisely. Logging into any Google service, such as YouTube or Gmail, for example, authenticates the user across all of Google's services. As a result, every Google platform that is launched in a new tab or browser instance shows the website that was just viewed, as well as the user's unique identity and avatar.

"The Google User ID is a Google-generated internal identity," the researchers noted. "It is the only way to identify a single Google account. It may be used with Google APIs to get the account owner's public personal information. Many variables influence the information exposed by these APIs. In most cases, the user's profile image is viewable at the very least."

Apart from not using Safari until a remedy is released, there isn't much users can do to prevent this vulnerability until one is released. On the plus side, Apple's designation of the problem as "resolved" means that a fix is on the way.