Researcher reveals ‘catastrophic’ security flaw in the Arc browser

Arc has a feature called Boosts that allows you to customize any website with custom CSS and Javascript. Since running arbitrary Javascript on websites has potential security concerns, we opted not to make Boosts with custom Javascript shareable across members, but we still synced them to our server so that your own Boosts are available across devices.

We use Firebase as the backend for certain Arc features (more on this below), and use it to persist Boosts for both sharing and syncing across devices. Unfortunately our Firebase ACLs (Access Control Lists, the way Firebase secures endpoints) were misconfigured, which allowed users Firebase requests to change the creatorID of a Boost after it had been created. This allowed any Boost to be assigned to any user (provided you had their userID), and thus activate it for them, leading to custom CSS or JS running on the website the boost was active on.

https://www.theverge.com/2024/9/20/24249919/arc-browser-boost-firebase-vulnerability-patched