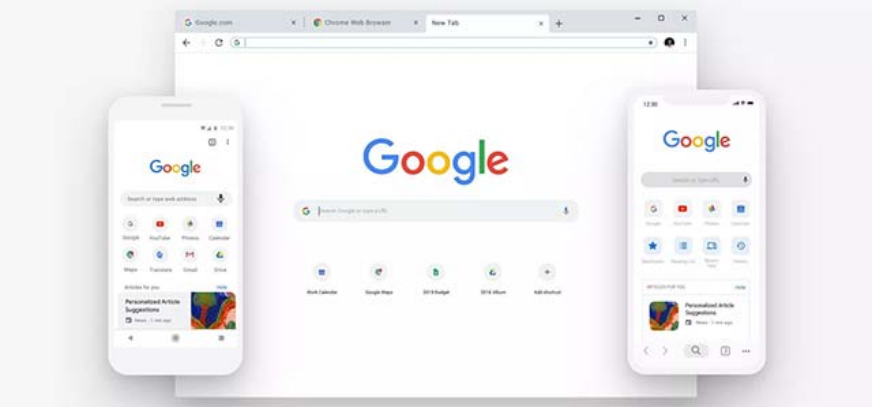
Chrome will support HTTP cache partitioning to prevent malicious attacks and unauthorized tracking

Google is planning to add a relatively new (relatively theoretically) new security feature to the Chrome web browser.

Google is planning to add a relatively new (relatively theoretically) new security feature to the Chrome web browser. This feature is called Cache Partitioning, designed to prevent potential malicious attacks as early as launching side-channel attacks, as well as secretly tracking user activity by abusing the browser's HTTP buffer.

Basically, this new feature will be responsible for partitioning Chrome's HTTP cache "by using top-frame origin (and also subframe origin) sources to prevent the documents from a specific source may disclose information about whether cross-origin is stored in the cache ".



1. Google Chrome 76: Safer mode, improved PWA and some other noticeable changes

Such an approach would effectively limit the inconvenience of an attacker to launch side-channel attacks, which use malicious websites that they control to detect whether a page Other websites that their target has access are in the web browser cache.

In the announcement of the introduction of 'Partition the HTTP Cache' feature, Google experts said the buffer attacks could trigger some of the following types of leak information:

1. **Detect and collect information about which site users have specifically visited:** If the resource is cached exclusively for a particular site or a specific group of websites, the attacker completes You can access the user's browsing history information by checking whether the buffer contains that resource.
2. T **cross-pressing between many different websites:** There is an existence of many types of website proofing attacks, in which hackers will take advantage of a common feature on websites (gmail, search

google .), that is automatically loading a specific image when the returned search result is blank. By opening a tab, performing a search, and then checking that image in the buffer, the crook can fully detect whether there is an arbitrary string in the search results. yours or not.

The browser cache can also be used as a method of 'taking fingerprints' by users by storing multi-site super cookies, requiring users to completely delete the browser cache if want to remove them.

1. Microsoft releases a new Windows 10 update, Microsoft Edge will be hidden if you install Edge Chromium

Attack abuses Chrome's HTTP buffer

An example of an HTTP buffer-based attack posted on this Github shows how a malicious agent can easily gather sensitive Chrome user information by abusing vulnerable endpoints. Google brand.

Cache Partitioning, designed to prevent potential malicious attacks early

Vulnerable sites that can be used in these attacks include important Google tools like Mail, Search, Books and even YouTube. Users will be redirected access to malicious websites, designed to trick victims into revealing sensitive information, as well as collect that information and send it to the attacker's server.

1. Incognito mode does not help you avoid Google's tracking algorithm when accessing adult websites

These types of data may fall into the hands of an attacker after a channel attack on the Chrome browser buffer is successfully implemented including:

1. Search history
2. Videos watched
3. The correct URLs are accessed
4. Time frame of activities
5. Private bookstore

6. Books read, purchased, marked, added to favorites .
7. Private email
8. Token, credit card number, phone number .
9. Frequency of sending emails
10. Information about email recipients
11. Directory (including email address, name, phone number)
12. Own notes
13. Bookmarked website (bookmark)
14. And many other related data

Necessary changes to prevent and limit buffer attacks

According to Google's description of the HTTP cache partitioning feature, the core solution here is 'top-frame source disk cache' of the page (for example, the information displayed in the address bar). or by combining sources of top-frame and sub-frame. In this way, resources loaded for a source can be read by another source and both issues will be resolved. "

1. Microsoft Edge Chromium has a feature that restricts videos from automatically playing, inviting experience

HTTP cache partitions can significantly restrict buffer attacks

Current options are used to isolate buffers and minimize buffer attacks:

1. (Source of top-frame, URL request) makes dual key
2. (Source of frame, required URL) makes double key
3. (Source of top-frame + source of frame, required URL) is a three-component key

"The Chrome team has been reluctant to solve this problem in the past due to concerns that the cache access rate will be significantly reduced, causing great pressure on network bandwidth usage and making the page load time longer, and recent tests in canary and dev channels show results that contradict our long-term thinking, there will be some small loss in performance, but very worth the trade off, 'said Google software engineer, Chrome developer Shivani Sharma.

Of all the most commonly used browsers, Safari is the only platform that has deployed the same version of the above mentioned HTTP cache feature (over 6 years ago). . In addition, Mozilla has recently implemented many new security enhancements. Meanwhile, Microsoft has not released any public signals about the plan to deploy the buffer partition in their Edge browser.

1. Mozilla launches a new browser called Firefox Preview, fast browsing speed and smooth running