Short-term Plan for Target Switching Bug of Puppeteer x Prerendering

This document is public

Author: alexrudenko@, dsv@, jrandolf@, kenoss@
Input from: nhiroki@, <yourname>@,
Status: Draft
Created: Apr 28, 2023
Last Updated: May 2, 2023

Note that alexrudenko@, dsv@ and jrandolf@ found and investigated this issue and kenoss@ is sorting out.

Objective

This document discusses a bug of Puppeteer and Prerender and a plan to fix it.

Bug

https://crbug.com/1440085

Recorder in DevTools doesn't work correctly if a replay triggers prerendering activation, e.g. DUI/DSE.

Preliminaries

- Prerender terminologies
  - Prerender2 with Multiple WebContents
  - [Public] Omnibox Trigger (Direct URL Input) for Prerendering (DUI)
  - Default search engine triggered Prerender2 (DSE)
- Recorder [blog] uses Puppeteer internally.
- Puppeteer uses a browser target and frame target. Not using tab target.
- Puppeteer is also used outside DevTools frontend.
- We are launching tab targets "Tab" targets in DevTools Protocol with the feature flag DevToolsTabTarget. As of 2023-04-29, our experiment is in Canary/Dev/Beta 50% and we are planning to launch at the end of 2023 May.
- Rest of the DevTools frontend supports tab targets, including the Preloading panel.

Root cause

A tab target is bound to a WebContents and manages (main frame?) frame targets under it. When a page is prerendered, we have a new FrameTree in the WebContents and a frame target. When prerender activated, prerendered FrameTree is migrated to the initiating one. To handle prerender activation correctly on the DevTools side, we need 1. Making the component in DevTools aware of tab targets. 2. Implementing switching logic for frame targets in the component. For example, see switching/handing over logic in the Preloading panel [simple switching] [handing over].

Observations:

A. If we want to allow prerendering in some DevTools component, we need DevToolsTabTarget.
B. Even if DevToolsTabTarget launched, we need additional implementation for Puppeteer. Note that we need to consider not only DevTools frontend, but other old DevTools clients.

Affected clients and components

- DevTools frontend
  - Recorder panel [blog]
  - Lighthouse
- Other clients
  - Puppeteer

Note that prerendering in other clients is rare at this timing, because possible trigger of prerendering is only SpeculationRules [github] and this is yet early adoption phase. On the other hand, Recorder and Lighthouse are affected because DUI/DSE triggers are (partially) enabled for Chrome.

Mitigation

In the long-term, presumably we need to make Puppeteer support prerendering. But it's not clear now. So, we discuss only short-term mitigation here.

For A, we'll launch DevToolsTabTarget as we planned.

For B, we'll disable prerendering in Recorder replay and DevTools client other than DevTools frontend as follows.

- Disable prerendering if a client connected with no tab target.
  - For DevTools frontend, prerendering is enabled. For other clients, disabled until they support tab targets.
  - Difficulty: Unknown. Need investigation. (Maybe dsv@ knows?)

- Implement a CDP command that enables/disables prerendering (browser-widely). Disable prerendering for Recorder replay invoking this CDP around it.
    - Difficulty: Easy. Prerender (preloading) is behind a feature flag, and has similar force-enable/disable logic already.

Note that the latter, DevTools frontend case, doesn’t depend on the DevToolsTabTarget. The former is a trick for other clients. So, the latter itself mitigates the situation and would take priority.

Note that it is not an option to disable prerendering if DevTools is connected because we need to support debug prerendering.