Web App Launch Handler: Security and Privacy self-review

Author: Alan Cutter
Last updated: 10 Nov 2022

Overview

This is the Security and Privacy self-review for the Web App Launch Handler manifest API.

Questions

2.1 What information might this feature expose to Web sites or other parties, and for what purposes is that exposure necessary?

This informs an installed web app that the user has launched the app via some launch mechanism such as via the start menu, a file handler, a share target, a captured link etc.

The target URL of the web app launch is included in the LaunchParams.

Any payloads associated with the launch (e.g. file handles) will be included in the LaunchParams as per their respective APIs. This spec doesn't control this content, just provides a container and delivery mechanism for it.

2.2. Do features in your specification expose the minimum amount of information necessary to enable their intended uses?

Yes.

2.3. How do the features in your specification deal with personal information, personally-identifiable information (PII), or information derived from them?

PII may be present in the launch payloads or target URLs however this information is not made newly available by this spec.

2.4. How do the features in your specification deal with sensitive information?

The only new information provided by this spec is whether a page load was due to a web app launch vs a regular browser navigation. This is not considered sensitive information.

2.5. Do the features in your specification introduce new state for an origin that persists across browsing sessions?

No, all involved data is ephemeral with the page used for the web app launch.

2.6. Do the features in your specification expose information about the underlying platform to origins?

No, the information provided is generic across all browser platforms.

2.7. Does this specification allow an origin to send data to the underlying platform?

No, the information flow is one way from the user agent to the page.

2.8. Do features in this specification enable access to device sensors?

No.

2.9. What data do the features in this specification expose to an origin? Please also document what data is identical to data exposed by other features, in the same or different contexts.

See 2.1 for the data exposed.
The target URL used for launch is already exposed to the origin via the network fetch.

2.10. Do features in this specification enable new script execution/loading mechanisms?

No, the consumer callback mechanism runs in the context of the document like regular scripts.

2.11. Do features in this specification allow an origin to access other devices?

No.

2.12. Do features in this specification allow an origin some measure of control over a user agent’s native UI?

Yes, this enables web apps to re-use existing app windows instead of spawning new ones. It also aims to in future enable web apps to select an existing app window to use via a service worker launch event.

2.13. What temporary identifiers do the features in this specification create or expose to the web?

None.

2.14. How does this specification distinguish between behavior in first-party and third-party contexts?

This API is only available to first party contexts.

2.15. How do the features in this specification work in the context of a browser's Private Browsing or Incognito mode?

Web apps are not supported in Incognito mode, this API does not apply.

2.16. Does this specification have both "Security Considerations" and "Privacy Considerations" sections?

Yes: https://wicg.github.io/web-app-launch/#priv-sec

2.17. Do features in your specification enable origins to downgrade default security protections?

No.

2.18. How does your feature handle non-"fully active" documents?

This feature only applies to active documents, a web app launch either spawns a new page or navigates/enqueues LaunchParams in an already active one.