

rrweb-io / rrweb Public[Code](#) [Issues 289](#) [Pull requests 114](#) [Actions](#) [Projects](#) [Security and quality](#)[New issue](#)

# [Bug]: DOM reconstruction may execute unintended scripts #1817

[Open](#)

Labels

[bug](#)

rotemreiss opened 2 weeks ago

[Contributor](#)

## Preflight Checklist

- I have searched the [issue tracker](#) for a bug report that matches the one I want to file, without success.

## What package is this bug report for?

rrweb-snapshot

## Version

1.0.0, &lt;= 2.0.0-alpha.18

## Expected Behavior

## Description

The `rebuild` method in **rrweb-snapshot** does not sufficiently sanitize snapshot data before reconstructing the DOM. This means that crafted content within a recorded session can cause unintended script execution when the session is replayed.

## Affected Versions

`rrweb-snapshot` `>= 1.0.0`, `<= 2.0.0-alpha.18` — no fixed version is available at the time of writing.

## Suggested Fix

---

Rendering the reconstructed DOM inside a **sandboxed iframe** (using the `sandbox` attribute) isolates the replayed content and prevents unintended scripts from running in the parent document's context.

If you are using rrweb in your application, **please ensure session replays are rendered inside a properly sandboxed iframe** until an official fix is released.

## Additional Context

---

I discovered this behavior approximately a year ago and reached out to the maintainers multiple times. The communication was acknowledged, but no fix has been provided or published as of today.

I also identified this issue in several real-world services that use rrweb for session replay. Their security teams were notified and have successfully remediated it by adjusting how they integrate rrweb in their applications.

A proof-of-concept is not being shared at this time to give the maintainers an opportunity to release a proper fix.

---

A CVE ID has been assigned for this issue ([CVE-2025-45806](#)) and is pending publication.

## Actual Behavior

N/A

## Steps to Reproduce

N/A

## Testcase Gist URL

*No response*

## Additional Information

*No response*



rotemreiss added bug [2 weeks ago](#)

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

## Metadata

### Assignees

No one assigned

### Labels

bug

### Type

No type

### Projects

No projects

### Milestone

No milestone

### Relationships

None yet

### Development

No branches or pull requests

### Participants



