# Unsafe inline XSS in pasting DOM element into chat

Low **gabek** published **GHSA-2hfj-cxw7-g45p** on Sep 26, 2021

Package

**chat.js** (n/a)

| Affected versions | Patched versions |
|---|---|
| 0.0.8 | 0.0.9 |

Description

## Impact

Inline scripts are executed when Javascript is parsed via a paste action.

1. Open https://watch.owncast.online/
2. Copy and then paste `<img src=null onerror=alert('hello')>` into the chat field.
3. An alert should pop up.

## Patches

```
    // Content security policy
    csp := []string{
        "script-src 'self' 'sha256-2HPCfJIJHnY0NrRDPTOdC7AOSJIcQyNxzUuut3TsYRY='",
        "worker-src 'self' blob:", // No single quotes around blob:
    }
```

Will be patched in 0.0.9 by blocking `unsafe-inline` Content Security Policy and specifying the `script-src`. The `worker-src` is required to be set to `blob` for the video player.

## For more information

If you have any questions or comments about this advisory:

- Open an issue in owncast/owncast
- Email us at gabek@real-ity.com

Severity

Low

CVE ID

CVE-2021-39183

Weaknesses

No CWEs

Credits

intrigus-lgtm