


 [octobercms](#) / [october](#) Public[Code](#) [Issues](#) 12 [Pull requests](#) 2 [Actions](#) [Security and quality](#) 43 

# Stored XSS via SVG Filter Bypass

Moderate [daftspunk](#) published [GHSA-gcqv-f29m-67gr](#) 2 weeks ago

## Package

*php* [october/rain](#) ([Composer](#)).

### Affected versions

`<=3.7.13, <=4.1.9`

### Patched versions

`3.7.14, 4.1.10`

## Description

A stored cross-site scripting (XSS) vulnerability was identified in the SVG sanitization logic. The regex pattern used to strip `on*` event handler attributes could be bypassed using a crafted payload that exploits how the pattern matches attribute boundaries.

## Impact

- Stored XSS via malicious SVG files uploaded through the Media Manager
- Could allow privilege escalation if a superuser views or embeds the malicious SVG
- Requires authenticated backend access with media upload permissions ( `media.library.create` )
- SVG must be viewed or embedded in a page to trigger

## Patches

The vulnerability has been patched in v3.7.14 and v4.1.10. All users are encouraged to upgrade to the latest patched version.

## Workarounds

If upgrading immediately is not possible:

- Disable SVG uploads by adding `svg` to the blocked extensions in media configuration
- Set `media.clean_vectors` to `true` in configuration (enabled by default)

## References

- Reported by Offensive Security Research Team

### Severity

Moderate

---

### CVE ID

CVE-2026-25133

---

### Weaknesses

No CWEs

---

### Credits



daftspunk

Remediation developer