Stored XSS in Backend Editor Markup Classes

Moderate **daftspunk** published **GHSA-6qmh-j78v-ffp7** 2 weeks ago

Package

php **october/system** (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 Backend Editor Settings. The Markup Classes fields (used for paragraph styles, inline styles, table styles, etc.) did not sanitize input to valid CSS class name characters. Malicious values were rendered unsanitized in Froala editor dropdown menus, allowing JavaScript execution when any user opened a RichEditor.

Impact

- Stored XSS via editor settings rendered in RichEditor dropdowns
- Could allow privilege escalation if a superuser opens any RichEditor (e.g., editing a blog post)
- Requires authenticated backend access with editor settings permissions
- Triggers on routine content editing operations

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:

- Restrict editor settings permissions to fully trusted administrators only

References

- Reported by Chris Alupului

Severity

Moderate

CVE ID

CVE-2026-24906

Weaknesses

No CWEs

Credits

 **Neosprings** Analyst

 **daftspunk** Remediation developer