System Settings (Social Media Management) Full Platform Compromise & Full Account Takeover for All-Roles & Privilege-Escalation via Stored DOM XSS

Moderate **bertugfahriozer** published **GHSA-gcfj-cf7j-vwgj** 5 days ago

Package

php **ci4-cms-erp/ci4ms** (Composer)

Affected versions	Patched versions
<= 0.28.6.0	0.31.0.0

Description

Summary

Vulnerability: Stored DOM XSS via System Settings – Social Media Management (Same-Page Attribute Breakout & Persistent Payload Injection)

- Stored Cross-Site Scripting via Unsanitized Social Media Configuration Fields with Immediate Same-Page Execution

Description

The application fails to properly sanitize user-controlled input within **System Settings – Social Media Management**. Multiple configuration fields, including **Social Media** and **Social Media Link**, accept attacker-controlled input that is stored server-side and later rendered without proper output encoding.

Unlike typical stored XSS that executes on other pages (such as public-facing landing pages), this vulnerability executes directly on the same settings page. The injected payload breaks out of the input attribute context and is immediately interpreted by the browser, resulting in same-page DOM-based XSS.

This represents a different functionality and a separate vulnerability class from public-facing landing page injection.

Affected Functionality

- System Settings – Social Media Management configuration
- Same-page rendering of user-controlled input fields
- DOM attribute injection within form inputs
- Storage and retrieval of social media configuration values

Attack Scenario

- An attacker injects a malicious JavaScript payload into one or more Social Media Management fields.
- The payload breaks out of the HTML attribute context.
- The application stores and re-renders the payload without sanitization or encoding.
- The payload executes immediately on the same settings page when rendered.
- The script executes in the browser context of the authenticated user managing settings.

Impact

- Persistent Stored XSS
- Immediate Same-Page DOM XSS execution
- Execution of arbitrary JavaScript in victims' browsers
- Administrative privilege escalation
- Full administrator account takeover
- Full account takeover across all roles
- Full compromise of the entire platform

Endpoints:

- `/backend/settings/` (Social Media Management)

Steps To Reproduce (POC)

1. Navigate to System Settings -> Social Media Management
2. Insert the following XSS payload into any Social Media or Social Media Link field:
   `test"><img src=1 onerror=alert()>" class="form-control" placeholder="Name" required>`
3. Save the settings
4. Observe that the payload breaks out of the input attribute context
5. The XSS executes immediately on the same page

Remediation

- Never use .html() again or any innerHTML-style like JS in your PHP, or any other sink, even if user inputs that flow into them are not clear, they still represent real world danger as an attacker can make use of this to exploit the application via XSS. And do HTML Encoding as much as possible and always do Sanitization, theres no sanitization there unfortunately. Also apply CSP, HttpOnly, SameSite, and Secure upon all application, they reduce severity of XSS & escalated-CSRF via XSS and do great jobs

Ready Video POC:

https://mega.nz/file/PBEFBCpJ#rGGxjnPN38qDtmJssAgIoLuStBcQaZFpR0J1bKAXApc

Severity

Moderate 4.7 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	Low

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

CVE ID

CVE-2026-34561

Weaknesses

▶ CWE-79

Credits

 **bugmithlegend** Reporter

 **LAW6ZX7** Reporter