# System Settings (Company Information) Full Platform Compromise & Full Account Takeover for All-Roles & Privilege-Escalation via Stored DOM XSS

Moderate **bertugfahriozer** published **GHSA-v897-c6vq-6cr3** 2 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 – Company Information (Same-Page Attribute Breakout & Persistent Payload Injection)

- Stored Cross-Site Scripting via Unsanitized Company Information Configuration Fields with Immediate Same-Page Execution

### Description

The application fails to properly sanitize user-controlled input within **System Settings – Company Information**. Several administrative configuration fields accept attacker-controlled input that is stored server-side and later rendered without proper output encoding.

Affected fields include, but are not limited to:

1. Company Name
2. Slogan

3. Company Phone
4. Company Mobile
5. Company Email
6. Google Maps iframe link
7. Company Logo and other media-related fields

Unlike the public-facing landing page injection vulnerability, this issue executes directly on the same settings page. The injected payload breaks out of the HTML attribute context and is immediately interpreted by the browser when rendered, resulting in same-page DOM-based stored XSS.

This represents different functionality and a separate vulnerability from public-facing rendering.

### Affected Functionality

- System Settings – Company Information configuration
- Same-page rendering of user-controlled input fields
- DOM attribute injection within form inputs
- Storage and retrieval of company information values

### Attack Scenario

- An attacker injects a malicious JavaScript payload into one or more Company Information 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.
- 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/` (Company Information)

## Steps To Reproduce (POC)

1. Navigate to System Settings -> Company Information

2. Insert the following XSS payload into any Company Information 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/qEcFUIjR#2OKX78JgPQI2x5957GE-vx1zYzJv2a9JqjyBsrRFBkk

**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-2026-34562

**Weaknesses**

▶ CWE-79

### Credits


**bugmithlegend** Reporter


**LAW6ZX7** Reporter