Menu Management (Pages) Full Account Takeover for All-Roles & Privilege-Escalation via Stored DOM XSS

Critical **bertugfahriozer** published **GHSA-g4pp-fhgf-8653** 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 Pages Added to Menu (Persistent Payload Injection)

- Stored Cross-Site Scripting via Unsafe Rendering of Page Entries in Menu Management

Description

The application fails to properly sanitize user-controlled input when **adding Pages to navigation menus** through the Menu Management functionality. Page-related data selected via the Pages section is stored server-side and rendered without proper output encoding.

This stored payload is later rendered unsafely within administrative interfaces and public-facing navigation menus, leading to stored DOM-based cross-site scripting (XSS).

Affected Functionality

- Menu Management – Pages section
- Adding pages to navigation menus

- Menu storage and rendering logic

Attack Scenario

- An attacker creates or controls a page containing a malicious JavaScript payload.
- The attacker adds the page to the menu using the **Pages** functionality in Menu Manager.
- The application stores the menu entry without sanitization or encoding.
- The payload persists and executes whenever the menu is rendered in administrative or public-facing interfaces.

Impact

- Persistent Stored DOM XSS
- Execution of arbitrary JavaScript in victims' browsers
- Privilege escalation when viewed by administrators or privileged users
- Full administrator account takeover
- Full account takeover across all roles via the navigation menu
- Full compromise of the entire application due to global execution in the navigation menu

Endpoint:

- `/backend/menu/`

Steps To Reproduce (POC)

1. Navigate to the **Menu Management** section of the application.
2. Use the **Pages** functionality to add a page containing an XSS payload such as:
   `<img src=x onerror=alert(document.domain)>`
3. Save the menu entry.
4. View the menu in the administrative panel or any public-facing page.
5. Observe the JavaScript payload executing automatically when the menu is rendered.

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/2c8lHSBQ#vwFDj0vhq7vLwMJjBjnAgbHWiIdFqUxAA913H_yQExQ

Severity

Critical 9.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-34564

Weaknesses

▶ CWE-79

Credits


bugmithlegend Reporter


peeefour Reporter