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

Moderate **bertugfahriozer** published **GHSA-66m2-v9v9-95c3** 4 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 – Mail Settings (Same-Page Attribute Breakout & Persistent Payload Injection)

- Stored Cross-Site Scripting via Unsanitized Mail Settings Configuration Fields

Description

The application fails to properly sanitize user-controlled input within **System Settings – Mail Settings**. Several configuration fields, including **Mail Server, Mail Port, Email Address, Email Password, Mail Protocol, and TLS settings**, accept attacker-controlled input that is stored server-side and later rendered without proper output encoding.

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

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

Example Affected Fields

- Mail Server: `test`
- Mail Port: `465`
- Email Address: `simple@gmail.com`
- Email Password: (any input)
- Mail Protocol: `SMTP`
- Domain: `simple@domain.com`

Affected Functionality

- System Settings – Mail Settings configuration
- Same-page rendering of user-controlled input fields
- DOM attribute injection within form inputs
- Storage and retrieval of mail configuration values

Attack Scenario

- An attacker injects a malicious JavaScript payload into one or more Mail Settings 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 Mail 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/` (Mail Settings)

Steps To Reproduce (POC)

1. Navigate to System Settings -> Mail Settings
2. Insert the following XSS payload into any Mail Settings 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() or any innerHTML-style sinks for user-controlled input in PHP or JavaScript.
- Apply proper **HTML encoding and input sanitization** for all configuration fields.
- Enforce CSP, HttpOnly, SameSite, and Secure flags for cookies to reduce the severity of XSS and potential CSRF escalation.
- Audit all other system settings fields for similar attribute injection vulnerabilities.

Ready Video POC:

https://mega.nz/file/KRNhUI6Q#NGC3Bow3RlnmdU1H2bGu1BGbpfIc-awi6IlvTp08V1s

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-2026-27599

Weaknesses

▶ CWE-79

Credits

bugmithlegend	Reporter
peeefour	Reporter
LAW6ZX7	Reporter