Stored XSS in Event Log Mail Preview

Moderate **daftspunk** published **GHSA-j4j5-9x6g-rgxc** 2 weeks ago

Package

php **october/system** (Composer)

Affected versions	Patched versions
<=3.7.13, <=4.1.9	3.7.14, 4.1.10

Description

A stored cross-site scripting (XSS) vulnerability was identified in the Event Log mail preview feature. When viewing logged mail messages, HTML content was rendered in an iframe without proper sandboxing, allowing JavaScript execution in the viewer's browser context.

Impact

- Stored XSS via mail template content rendered in Event Log
- Could allow privilege escalation if a superuser views a malicious log entry
- Requires authenticated backend access with mail template editing permissions
- Requires a superuser to view the specific Event Log entry to trigger

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 mail template editing permissions to fully trusted administrators only
- Restrict Event Log viewing permissions to minimize exposure

References

- Reported by Chris Alupului

Severity

Moderate

CVE ID

CVE-2026-24907

Weaknesses

No CWEs

Credits

 **Neosprings** Analyst

 **daftspunk** Remediation developer