Page creation API bypasses `changeStatus` permission check via unfiltered `isDraft` parameter

Moderate **bastianallgeier** published **GHSA-w942-j9r6-hr6r** 2 days ago

Package

php **getkirby/cms** (Composer)

Affected versions

<=4.8.0, 5.0.0-5.3.3

Patched versions

4.9.0, 5.4.0

Description

TL;DR

This vulnerability affects all Kirby sites where users have the permission to create pages (`pages.create` permission is enabled) but not the permission to change the status of pages (`pages.changeStatus` permission is disabled). This can be due to configuration in the user blueprint(s), via `options` in the page blueprint(s) or via a combination of both settings.

Your Kirby sites are *not* affected if your use case does not consider the creation of published pages a malicious action. The vulnerability can only be exploited by authenticated users.

Introduction

An authorization bypass allows authenticated users to perform actions they should not be allowed to perform based on their configured permissions, thereby causing a privilege escalation.

The effects of an authorization bypass can include unauthorized access to sensitive information as well as unauthorized changes to content or system information.

Impact

Kirby's user permissions control which user role is allowed to perform specific actions to content models in the CMS. These permissions are defined for each role in the user blueprint (`site/blueprints/users/...`). It is also possible to customize the permissions for each target model in the model blueprints (such as in `site/blueprints/pages/...`) using the `options` feature. The permissions and options together control the authorization of user actions.

For pages, Kirby provides the `pages.create` and `pages.changeStatus` permissions (among others). In affected releases, Kirby checked these permissions independently and only for the respective action. However the `changeStatus` permission didn't take effect on page creation.

New pages are created as drafts by default and need to be published by changing the page status of an existing page draft. This is ensured when the page is created via the Kirby Panel. However the REST API allows to override the `isDraft` flag when creating a new page. This allowed authenticated attackers with the `pages.create` permission to immediately create published pages, bypassing the normal editorial workflow.

Patches

The problem has been patched in Kirby 4.9.0 and Kirby 5.4.0. Please update to one of these or a later version to fix the vulnerability.

In all of the mentioned releases, we have added a check to the page creation rules that ensures that users without the `pages.changeStatus` permission cannot create published pages, only page drafts.

Credits

Thanks to **@offset** for responsibly reporting the identified issue.

Severity

Moderate 5.3 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	None

Vulnerable System Impact Metrics

Confidentiality	None
Integrity	Low
Availability	None

Subsequent System Impact Metrics

Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

CVE ID

CVE-2026-40099

Weaknesses

▶ CWE-863

Credits

offset Reporter