

 octobercms / **october** Public[Code](#) [Issues](#) 12 [Pull requests](#) 2 [Actions](#) [Security and quality](#) 43 

# Twig Sandbox Bypass via Collection Methods

Moderate daftspunk published **GHSA-m5qg-jc75-4jp6** 2 weeks ago

## Package

*php* **october/rain** ([Composer](#))

## Affected versions

`<=3.7.12, <=4.1.4`

## Patched versions

`3.7.13, 4.1.5`

## Description

A sandbox bypass vulnerability was identified in the optional Twig safe mode feature ( `CMS_SAFE_MODE` ). Certain methods on the `collect()` helper were not properly restricted, allowing authenticated users with template editing permissions to bypass sandbox protections.

## Impact

- Bypass of Twig sandbox restrictions
- Only affects installations with `CMS_SAFE_MODE` enabled (disabled by default)
- Requires authenticated backend access with CMS template editing permissions

## Patches

The vulnerability has been patched in v4.1.5 and v3.7.13. All users who have enabled safe mode are encouraged to upgrade to the latest patched version.

## Workarounds

If upgrading immediately is not possible:

- Disable `CMS_SAFE_MODE` if untrusted template editing is not required
- Restrict CMS template editing permissions to fully trusted administrators only

## References

- Reported by Łukasz Rybak

### Severity

Moderate 4.9 / 10

#### CVSS v3 base metrics

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

[Learn more about base metrics](#)

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

### CVE ID

CVE-2026-22692

### Weaknesses

No CWEs

### Credits

 **lukasz-rybak**

Analyst

 **daftspunk**

Remediation developer