


 [octobercms](#) / [october](#) Public[Code](#) [Issues](#) 12 [Pull requests](#) 1 [Actions](#) [Security and quality](#) 39 

# Environment Variable Exfiltration via INI Parser Interpolation

Moderate [daftspunk](#) published [GHSA-g6v3-wv4j-x9hg](#) 16 hours ago

## Package

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

## Affected versions

`<=3.7.13, <=4.1.9`

## Patched versions

`3.7.14, 4.1.10`

## Description

A server-side information disclosure vulnerability was identified in the INI settings parser. PHP's `parse_ini_string()` function supports `${}` syntax for environment variable interpolation. Attackers with Editor access could inject `${APP_KEY}`, `${DB_PASSWORD}`, or similar patterns into CMS page settings fields, causing sensitive environment variables to be resolved and stored in the template. These values were then returned to the attacker when the page was reopened.

## Impact

- Exfiltration of sensitive environment variables (APP\_KEY, DB credentials, AWS keys, etc.)
- Could enable further attacks: database access, cookie forgery, AWS resource access
- Requires authenticated backend access with Editor permissions
- Only relevant when `cms.safe_mode` is enabled (otherwise direct PHP injection is already possible)

## 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 Editor tool access to fully trusted administrators only

- Ensure database and cloud service credentials are not accessible from the web server's network

## References

- Reported by Proactive Testing Team (PTT)

### 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-2026-25125

### Weaknesses

No CWEs

### Credits



daftspunk

Remediation developer