Safe Mode Bypass via CSS Preprocessor Compilers

Moderate **daftspunk** published **GHSA-3888-q23f-x7qh** 4 days ago

Package

php **october/system** (Composer)

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

Description

A server-side information disclosure vulnerability was identified in the handling of CSS preprocessor files. Backend users with Editor permissions could craft `.less`, `.sass`, or `.scss` files that leverage the compiler's import functionality to read arbitrary files from the server. This worked even with `cms.safe_mode` enabled.

Impact

- Potential exposure of sensitive server-side files
- 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. When `cms.safe_mode` is enabled, `.less`, `.sass`, and `.scss` files can no longer be created, uploaded, or edited across the CMS editor, media manager, and file upload interfaces. All users are encouraged to upgrade to the latest patched version.

Workarounds

If upgrading immediately is not possible:

- Set `cms.editable_asset_types` config to `['css', 'js']` to remove preprocessor file types from the editor

- Restrict Editor tool access to fully trusted administrators only

References

- Reported by Chris Alupului

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-2026-26067

Weaknesses

No CWEs

Credits

Neosprings	Finder
daftspunk	Remediation developer