Safe Mode Bypass via Twig Database Write Operations

Moderate **daftspunk** published **GHSA-h6jm-f4hh-fw27** 9 hours ago

Package

php **october/system** (Composer)

Affected versions

<=3.7.13, <=4.1.9

Patched versions

3.7.14, 4.1.10

Description

A vulnerability was identified in the Twig sandbox security policy that allowed database write operations when `cms.safe_mode` is enabled. Backend users with Developer permissions could use Twig template markup to execute insert, update, and delete operations on any database table through the query builder, which is included in the sandbox allow-list.

Impact

- Arbitrary database writes including modification or deletion of any table
- Requires authenticated backend access with Developer 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. Write operations such as `insert`, `update`, `delete`, and `truncate` are now blocked on query builder and model objects within the Twig sandbox. All users are encouraged to upgrade to the latest patched version.

Workarounds

If upgrading immediately is not possible:

- Restrict Developer tool access to fully trusted administrators only

References

- Reported by Chris Alupului

Severity

Moderate 6.6 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-26274

Weaknesses

No CWEs

Credits

 **Neosprings** Finder

 **daftspunk** Remediation developer