XENFORO / OAUTH2 · 08 SEPT 2026

CVE-2026-73309: Empty OAuth2 credentials bypass

Empty PKCE verifiers and client secrets bypassed OAuth2 credential checks.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

XenForo 2.3.12 build 2031270 accepted empty OAuth2 credentials at the token endpoint. An empty PKCE verifier allowed an authorization code to be redeemed without proving possession of the original verifier. Empty client secrets affected authorization-code and refresh-token grants through the same code pattern.

Technical details

The token endpoint called `assertRequiredApiInput()`, which checked that the parameter existed but did not require a non-empty value. Credential verification was then guarded by truthiness checks:

```
if ($input['client_secret']) { /* compare it */ }
if ($input['code_verifier']) { /* verify PKCE */ }
```

PHP evaluates both `''` and `'0'` as false, so either value bypassed the comparison block.

duction

Skip to debugger view

000000000042845D
000000000042848B
000000000042848E
00000000004284FF
0000000000428567
00000000004285AC
00000000004285B6
00000000004285C9
00000000004285CC
00000000004285DE

1. Complete a normal S256 authorization flow for a public OAuth2 client and capture the authorization code.
2. Exchange the code at the token endpoint with `code_verifier=` instead of the verifier used to create the challenge.
3. Use the returned access token to request `/api/me`.

The server returned access and refresh tokens, and `/api/me` accepted the access token. Supplying an incorrect non-empty verifier caused the exchange to fail.

Impact

Anyone who obtained a live authorization code for a public client could redeem it without the PKCE verifier. The issued tokens retained the user-approved scopes. Exploitation still required a valid authorization code.

XenForo 2.3.13 rejects empty credentials before processing the grant.

References

- CVE-2026-73309
- PoC
- VulnCheck advisory
- XenForo 2.3.13 release

0000000000428000 · 25 RENDERED LINES · 1888 UTF-8 BYTES IN .WEB.OAUTH

.WEB.OAUTH · ADDRESSES ARE UTF-8 BYTE OFFSETS

AU: IDLE VIEW: POST VIEW