XENFORO / OAUTH2 · 08 SEPT 2026

CVE-2026-73310: OAuth2 redirect URI mismatch

An OAuth code issued for callback A could be redeemed with callback B.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

000000000428800
000000000428894
0000000004288F5
000000000428906
00000000042898B
000000000428A14
000000000428A24
000000000428A30
000000000428A6B
000000000428A85
000000000428ABA
000000000428ADC
000000000428B53

XenForo 2.3.12 build 2031270 did not bind an OAuth2 authorization code to the redirect URI used during authorization. A code issued for one registered callback could be redeemed through another callback registered to the same client.

Technical details

XenForo stored the selected redirect URI on the `OAuthRequest`. During token redemption, the server only checked whether the submitted `redirect_uri` appeared in the client's allowlist. It did not compare that value with the URI attached to the authorization request that issued the code.

Reproduction

1. Register callback A and callback B on the same client.
2. Authorize with callback A.
3. Exchange the resulting code while sending callback B.

Skip to debugger view

the returned token at `/api/me`.

00000000000428C5E

00000000000428C7B

The token endpoint returned an access token, and the token authenticated as the user who authorized through callback A.

00000000000428CDF

Impact

00000000000428CE9

An attacker with a valid authorization code and control of another registered callback could redeem the code through that callback. Relevant cases include abandoned endpoints and custom URI schemes claimed by another application. The attack does not bypass the requirement for a valid code.

00000000000428CFC

00000000000428CFF

00000000000428D11

Xenforo 2.3.13 binds the submitted redirect URI to the authorization request that produced the code.

References

- CVE-2026-73310
- PoC
- VulnCheck advisory
- Xenforo 2.3.13 release

0000000000428800 · 22 RENDERED LINES · 1679 UTF-8 BYTES IN .WEB.OAUTH

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

AU: IDLE VIEW: POST VIEW