XENFORO / OAUTH2 · 08 SEPT 2026

CVE-2026-73311: OAuth2 authorization code replay

The same XenForo OAuth authorization code could be redeemed more than once.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

00000000000428F00
00000000000428F96
00000000000428FC5
00000000000428FD6
00000000000429062
00000000000429126
00000000000429251

XenForo 2.3.12 build 2031270 allowed the same OAuth2 authorization code to be redeemed more than once. Each successful exchange created a separate access token and refresh-token family.

Technical details

`grantAuthorizationCode()` loaded the code, checked `isValid()` and created the tokens. It then returned the response without deleting the code or marking it as used. Two simultaneous requests could also pass the validity check before either one finished.

00000000004290D1
00000000004290DD
00000000004291AB
00000000004291D0

Reproduction

1. Complete an OAuth2 authorization flow and capture the token request.
2. Send the request once and record the returned access and refresh tokens.
3. d the same request again with the same authorization code.

Skip to debugger view

000000000042934 1

4. Verify both access tokens at `/api/me`.

000000000042938 9

Both exchanges returned HTTP 200. The responses contained different access tokens and different refresh tokens for the same user.

000000000042938 3

000000000042938 6

Impact

000000000042938 9

Anyone able to capture a complete valid token request could replay it until the authorization code expired. Client authentication and PKCE material remained required where applicable. Every replay created another refresh-token family.

000000000042938 B

XenForo 2.3.13 consumes the authorization code while issuing tokens, including for concurrent exchanges.

References

- CVE-2026-73311
- PoC
- VulnCheck advisory
- XenForo 2.3.13 release

000000000042 8F00 · 20 RENDERED LINES · 1597 UTF-8 BYTES IN .WEB.OAUTH

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

AU: IDLE VIEW: POST VIEW