XENFORO / OAUTH2 · 08 SEPT 2026

CVE-2026-73312: Refresh token replay after access-token expiry

An expired XenForo access token left its refresh token reusable.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

000000000042960D
000000000042967E
00000000004296D4
00000000004296E5
0000000000429759
00000000004297CB
00000000004297E1
000000000042981C
0000000000429828
0000000000429867
000000000042988B
00000000004298C4
00000000004298EC
000000000042991A

XenForo 2.3.12 build 2031270 allowed a refresh token to be reused after its associated access token expired. Each replay issued a new access-token and refresh-token pair with the same user and scopes.

Technical details

The refresh endpoint created the replacement pair and then called the old access token's revocation routine. That routine started by checking whether the access token was still valid. An expired token failed immediately, so the function returned before revoking anything-including the related refresh token.

Reproduction

1. Obtain a valid OAuth2 access token and its refresh token.
2. Wait for the access token to expire.
3. Submit the refresh token and record the replacement pair.
4. Submit the original refresh token again.
5. Verify both returned access tokens at `/api/me`.

Skip to debugger view

00000000000429970
00000000004299E2
00000000000429A1A
00000000000429A8A
00000000000429A99
00000000000429AA3
00000000000429AB6
00000000000429AB9
00000000000429ACB

Both refresh requests succeeded, and the original refresh token remained usable.

Impact

Anyone holding the refresh token could continue creating valid token pairs after the parent access token expired. Confidential clients still required their client secret.

XenForo 2.3.13 consumes the refresh token independently of its expired parent and issues the replacement in the same operation.

References

- CVE-2026-73312
- PoC
- VulnCheck advisory
- XenForo 2.3.13 release

00000000000429600 · 23 RENDERED LINES · 1592 UTF-8 BYTES IN .WEB.OAUTH

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

AU: IDLE VIEW: POST VIEW