XENFORO / AUTHENTICATION · 08 SEPT 2026

CVE-2026-73313: Passkey accepted for the wrong account

A passkey from one XenForo account completed another account's pending login.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

00000000042A000
00000000042A07F
00000000042A0D9
00000000042A0EA
00000000042A15B
00000000042A1C8
00000000042A20C
00000000042A218
00000000042A23D
00000000042A26F
00000000042A29F
00000000042A2D9

XenForo 2.3.12 build 2031270 accepted a valid passkey assertion from one user to complete another user's pending two-step login. The issue affected both the public login flow and the admin control panel.

Technical details

The passkey manager found the credential globally and verified the challenge, origin, RP ID, signature, presence flag and counter. All of that was correct. The credential record also had the owner's `user_id`, but the TFA provider never compared it with the account waiting to finish login.

Reproduction

1. Register a passkey on account A.
2. Enable passkey two-step verification on account B.
3. Start a login for account B with B's password.
4. plete the passkey prompt with account A's credential.

Skip to debugger view

00000000042A3BD

00000000042A41F

00000000042A479

00000000042A483

00000000042A496

00000000042A499

00000000042A4AB

XenForo accepted the assertion and opened a session for account B. The same sequence completed an ACP login.

Impact

An attacker who knew the target account's password could satisfy its passkey-based second factor with a passkey registered to another account. The attacker needed control of that second account and its passkey.

XenForo 2.3.13 verifies that the credential owner matches the account being authenticated.

References

- CVE-2026-73313
- PoC
- VulnCheck advisory
- XenForo 2.3.13 release

00000000042A000 · 21 RENDERED LINES · 1539 UTF-8 BYTES IN .WEB.AUTH

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

AU: IDLE VIEW: POST VIEW