XENFORO / AUTHORIZATION · 08 SEPT 2026

CVE-2026-73318: Missing permission checks on agreement resets

A restricted ACP administrator could reset the board's agreement timestamps.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

00000000042CC00
00000000042CC96
00000000042CD16
00000000042CD24
00000000042CD35
00000000042CDBB
00000000042CDC3
00000000042CE38
00000000042CE44
00000000042CE83
00000000042CEDE
00000000042CF26
00000000042CF72
00000000042CFF9

Xenforo 2.3.12 build 2031270 allowed a restricted admin control panel user without the `option` permission to reset the board-wide privacy-policy and terms acceptance timestamps. The affected actions returned HTTP 200 even though their controls were hidden from that administrator.

Technical details

The ACP navigation checked `option` before showing the controls. `ForceAgreementController` never repeated that check when it handled the request.

The routes update global agreement timestamps. Moving either timestamp forward invalidates every existing acceptance.

Reproduction

1. Create an ACP administrator without the `option` permission.
2. Log in as that administrator and confirm that the agreement-et controls are unavailable.

Skip to debugger view

00000000042CFFF
00000000042D087
00000000042D0B1
00000000042D0EF
00000000042D0F9
00000000042D108
00000000042D10B
00000000042D11D

3. Send direct POST requests to the privacy-policy and terms reset actions.
4. Read the global agreement timestamps and open the board as an existing user.

Both requests returned HTTP 200 and advanced the corresponding timestamps. Existing users were required to accept the agreements again.

Impact

A restricted ACP administrator could force every board user to repeat the privacy-policy or terms acceptance flow, causing a board-wide interruption until each user completed it.

XenForo added the controller-level permission check in 2.3.13.

References

- CVE record
- PoC
- VulnCheck advisory
- XenForo 2.3.13 release

00000000042CC00 · 22 RENDERED LINES · 1687 UTF-8 BYTES IN .WEB.AUTHZ
.WEB.AUTHZ · ADDRESSES ARE UTF-8 BYTE OFFSETS

AU: IDLE VIEW: POST VIEW