XENFORO / AUTHORIZATION · 08 SEPT 2026

CVE-2026-73317: ACP rebuild authorization bypass

A restricted ACP administrator could launch an approval job as another user.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

00000000042C400
00000000042C480
00000000042C4EC
00000000042C51E
00000000042C52F
00000000042C599
00000000042C609
00000000042C677
00000000042C6E9
00000000042C6F2
00000000042C6FE
00000000042C747
00000000042C77F

Xenforo 2.3.12 build 2031270 allowed a restricted admin control panel user with the `rebuildCache` permission to run an approval-queue job as another user. The restricted administrator could approve a pending account despite receiving HTTP 403 from the normal approval route.

Technical details

The controller accepted a job class and its options, checked `rebuildCache` plus manual-trigger support and dispatched it. `XF:ApprovalQueueProcess` happened to be manually triggerable, and one of its options was `asUserId`.

`ToolsController::actionRebuild()` did not check whether the administrator had permission to perform the action implemented by the selected job. The request controlled both the job class and the user identity supplied through `asUserId`.

Reproduction

Skip to debugger view

00000000042C84F

00000000042C87A

00000000042C8E6

00000000042C8EC

00000000042C957

00000000042C982

00000000042C9BA

00000000042C9C4

00000000042C9D3

00000000042C9D6

00000000042C9E8

1. Create an ACP administrator with only the cache-rebuild permission.
2. Create or identify a user waiting in the approval queue.
3. Confirm that the restricted administrator receives HTTP 403 from the normal approval action.
4. Submit `XF:ApprovalQueueProcess` through the rebuild endpoint with the target account and a privileged `asUserId` value.
5. Check the target account and moderator log.

The job approved the account. The moderator log attributed the action to the user supplied through `asUserId`.

Impact

A restricted ACP administrator could execute approval-queue actions outside their assigned permissions and attribute those actions to another account.

XenForo restricted the rebuild-job dispatcher in 2.3.13.

References

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

00000000042C400 · 26 RENDERED LINES · 1905 UTF-8 BYTES IN .WEB.AUTHZ

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

AU: IDLE VIEW: POST VIEW