XENFORO / INFORMATION DISCLOSURE · 08 SEPT 2026

CVE-2026-73320: Unauthenticated unfurl result disclosure

Sequential result IDs exposed stored link previews without authentication.

000000000436700
000000000436778
0000000004367EC
000000000436810
000000000436820
000000000436890
0000000004368D4
0000000004368E0
000000000436930
000000000436976
000000000436990
0000000004369C2
0000000004369DE

Xenforo 2.3.12 build 2031270 returned stored link-preview results from `unfurl.php` without requiring a XenForo session. A numeric `UnfurlResult` ID was sufficient to retrieve the preview HTML and source URL, including results created from restricted posts and conversations.

Technical details

`UnfurlResult` IDs were global and sequential. The endpoint returned the referenced result without checking whether the requester could view the content that created it.

Reproduction

1. Submit a standalone URL in content you control and record its `UnfurlResult` ID.
2. Create a link preview in restricted content and note its result ID.
3. Remove all XenForo cookies.
4. Request the nearby result IDs through `unfurl.php`:

Skip to debugger view

000000000436A4C
000000000436A52
000000000436AC3
000000000436B2E
000000000436B7B
000000000436BA4
000000000436BAE
000000000436BBD
000000000436BC0
000000000436BD2

```
GET /unfurl.php?result=<id>
GET /unfurl.php?result=<adjacent-id>
```

The cookie-less request returned the preview HTML and its full source URL.

Impact

An unauthenticated requester could enumerate recent result IDs and read preview data generated from content they could not access. Exploitation depended on guessing a live result before it expired, and useful disclosure depended on the target content containing a standalone URL with preview data.

XenForo protected the endpoint in 2.3.13.

References

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

0000000000436700 · 24 RENDERED LINES · 1632 UTF-8 BYTES IN .WEB.INFO
.WEB.INFO · ADDRESSES ARE UTF-8 BYTE OFFSETS

AU: IDLE VIEW: POST VIEW