XENFORO / XSS · 08 SEPT 2026

CVE-2026-73319: JavaScript URI in dynamic redirects

A JavaScript URI passed same-host validation and executed after a confirmed redirect.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

0000000000432300
0000000000432396
00000000004323F2
0000000000432403
000000000043248C
00000000004324B0
00000000004324E9
0000000000432573
00000000004325E1
00000000004325ED
0000000000432641
0000000000432682

Xenforo 2.3.12 build 2031270 accepted a `javascript:` URI as a same-host redirect target. A logged-in user who opened an attacker-prepared Follow confirmation link and confirmed the action executed JavaScript in the XenForo origin.

Technical details

The redirect validator used PHP's URL parser to compare the supplied host with the board host but did not restrict the URI scheme. The following payload passed that check:

```
javascript://board.example/%0Awindow.name='marker';void 0
```

PHP parsed `board.example` as the host, so XenForo's same-host check accepted it. The browser treated everything after `//` as a JavaScript comment. `%0A` ended the comment, and the remaining code ran when XenForo assigned the value to `window.location`.

Reproduction

Skip to debugger view

000000000004326F1
000000000004326F7
000000000043277E
000000000004327BB
000000000004327EA
000000000004327F4
000000000043280 3
000000000043280 6
000000000043281 8

1. Serve a Follow confirmation URL whose return target contains the payload above.
2. Open the link in a browser with an authenticated XenForo session.
3. Confirm the Follow action.
4. The browser executes the JavaScript in the XenForo origin as it follows the redirect.

Impact

An attacker could execute JavaScript in the context of a logged-in XenForo user who opened the prepared link and confirmed the action. The payload ran with the user's access to the board origin.

XenForo limited the accepted schemes in 2.3.13.

References

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

0000000000432300 · 22 RENDERED LINES · 1670 UTF-8 BYTES IN .WEB.XSS

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

AU: IDLE VIEW: POST VIEW