XENFORO / DENIAL OF SERVICE · 08 SEPT 2026

CVE-2026-73321: Stack overflow in BBCode parsing

Five thousand nested quote tags terminated a XenForo PHP worker with a stack overflow.

000000000043700 0
000000000043708 1

Xenforo 2.3.12 build 2031270 recursively parsed deeply nested BBCode before enforcing its effective depth limit. A guest request containing 5,000 nested `[quote]` tags caused the PHP worker to terminate with a stack overflow.

000000000043708 E
000000000043716 F

Technical details

000000000043716 F
000000000043724 D

The parser already had a maximum-depth setting, but opening tags accumulated recursively before Xenforo enforced it. Normal message-length validation also happened after the parser had built and walked the nested structure.

000000000043724 A

The approximately 75 KB trigger repeated the following structure 5,000 times:

000000000043725 A
000000000043726 6

```
[quote][quote][quote]...[/quote][/quote][/quote]
```

000000000043726 B
000000000043727 E

Reproduction

000000000043733 E

erate 5,000 nested opening `[quote]` tags followed by the matching closing tags.

Skip to debugger view

0000000000437DA
0000000000437E0
0000000000437452
0000000000437A3
0000000000437F0
0000000000437FA
0000000000437509
000000000043750C
000000000043751E

2. Submit the payload to the guest-accessible BBCode-to-HTML endpoint.
3. Monitor the HTTP response, Apache error log, and worker process.

The request terminated the PHP worker with Windows status `0xC00000FD`, the stack-overflow exception. Apache logged the exit and started a replacement worker.

Impact

An unauthenticated requester could terminate a PHP worker with one request. Concurrent requests could temporarily consume the available worker pool while Apache replaced the terminated processes.

XenForo moved the effective depth limit ahead of recursive parsing in 2.3.13.

References

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

0000000000437000 · 22 RENDERED LINES · 1690 UTF-8 BYTES IN .WEB.DOS
.WEB.DOS · ADDRESSES ARE UTF-8 BYTE OFFSETS
AU: IDLE VIEW: POST VIEW