XENFORO / PAYMENTS · 08 SEPT 2026

CVE-2026-73316: PayPal webhook replay

XenForo processed the same signed PayPal callback more than once.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

00000000042E700
00000000042E77D
00000000042E7EC
00000000042E7FF
00000000042E810
00000000042E884
00000000042E8EE
00000000042E95A
00000000042E971
00000000042E97D
00000000042E9B7
00000000042E9D0
00000000042E9FE
00000000042EA6E
00000000042EA76

XenForo 2.3.12 build 2031270 processed the same authenticated PayPal REST webhook more than once. Replaying one signed payment-completion callback created duplicate transaction records and extended the associated recurring user upgrade twice.

Technical details

XenForo's base payment code already checks whether a provider transaction was processed. The PayPal REST override of `validateTransaction()` skipped that implementation, and the database accepted duplicate transaction IDs.

Once signature verification passed, purchase completion ran without checking whether the provider event had already been processed.

Reproduction

1. Send the callback once and record the new expiry date.
2. lay the exact request.
3. Compare the payment log and expiry date again.

Skip to debugger view

00000000042EA7C

00000000042EAEF

00000000042EB4C

00000000042EB82

00000000042EB8C

00000000042EB9B

00000000042EB9E

00000000042EBB0

Both requests succeeded. XenForo logged the same provider transaction twice and extended the upgrade after each request.

Impact

Anyone able to capture one authentic callback with its original signature could replay that callback to repeat its payment-side effect. For recurring user upgrades, each replay extended the expiry date again.

XenForo added transaction replay protection in 2.3.13.

References

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

00000000042E700 · 23 RENDERED LINES · 1562 UTF-8 BYTES IN .WEB.PAY

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

AU: IDLE VIEW: POST VIEW