XENFORO / PAYMENTS · 08 SEPT 2026

CVE-2026-73314: PayPal signature check bypass

An unsupported PayPal signature algorithm caused webhook verification to return success.

00000000042E000
00000000042E08C
00000000042E0EE
00000000042E0FF
00000000042E18D
00000000042E213
00000000042E219
00000000042E231
00000000042E262
00000000042E26E
00000000042E2A7
00000000042E2EC
00000000042E377

Xenforo 2.3.12 build 2031270 treated an unsupported PayPal webhook signature algorithm as a successful verification. A forged `PAYMENT.CAPTURE.COMPLETED` callback extended a recurring user upgrade without a PayPal signing key.

Technical details

`PayPalRest::verifyWebhookSignature()` mapped `PAYPAL-AUTH-ALGO` through an allowlist containing `SHA256withRSA`. An unknown value left the OpenSSL algorithm unset. That branch logged that verification had been skipped and returned `true`, allowing the webhook handler to process the event.

The relevant header was:

```
PAYPAL-AUTH-ALGO: definitely-not-a-real-algorithm
```

Reproduction

ate an active PayPal REST recurring user upgrade.

Skip to debugger view

00000000042E3FF

2. Build a `PAYMENT.CAPTURE.COMPLETED` callback for that purchase context.

00000000042E434

3. Set `PAYPAL-AUTH-ALGO` to an unsupported value and send the callback without a valid PayPal signature.

00000000042E43A

00000000042E4C1

4. Check the user's upgrade expiry date.

00000000042E4CB

The callback returned success and extended the recurring upgrade by 30 days. The purchase values used by the callback were available to the buyer through the upgrade and cancellation flows.

00000000042E524

00000000042E52E

00000000042E53D

Impact

00000000042E540

A buyer could forge a completed-payment callback for their purchase context and extend the related user upgrade without a valid PayPal signature.

00000000042E552

Xenforo 2.3.13 rejects unsupported algorithms and unavailable cryptographic verification.

References

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

00000000042E000 · 24 RENDERED LINES · 1758 UTF-8 BYTES IN .WEB.PAY

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

AU: IDLE VIEW: POST VIEW