XENFORO / SSRF · 08 SEPT 2026

CVE-2026-73315: PayPal certificate URL SSRF

A PayPal webhook header triggered an HTTP or HTTPS request to an attacker-selected URL.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

00000000042F000
00000000042F078
00000000042F0E5
00000000042F0F6
00000000042F163
00000000042F1A7
00000000042F1D9
00000000042F24A
00000000042F288
00000000042F294
00000000042F2DA
00000000042F32A
00000000042F360

XenForo 2.3.12 build 2031270 fetched the URL supplied in the PayPal `PAYPAL-CERT-URL` webhook header without restricting its destination. The request was issued before the callback's signature had been authenticated.

Technical details

The PayPal REST webhook handler passed `PAYPAL-CERT-URL` directly to its HTTP client. HTTP and HTTPS URLs were accepted, including private addresses and hosts unrelated to PayPal.

```
PAYPAL-CERT-URL: https://listener.example/cert.pem
```

XenForo sent the GET request before parsing the response as a certificate. Invalid certificate data caused later verification to fail but did not prevent the outbound request.

Reproduction

1. Start an HTTP or HTTPS listener reachable from the XenForo
ver.

Skip to debugger view

00000000042F3D4
00000000042F40F
00000000042F442
00000000042F44C
00000000042F45B
00000000042F45E
00000000042F470

2. Send a PayPal REST webhook request with `PAYPAL-CERT-URL` set to the listener URL.
3. Observe the inbound GET request from the XenForo host.

Impact

An unauthenticated webhook request could make the XenForo server issue HTTP or HTTPS GET requests to attacker-selected destinations, including private network addresses.

XenForo restricted certificate retrieval in 2.3.13.

References

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

00000000042F000 · 21 RENDERED LINES · 1503 UTF-8 BYTES IN .WEB.SSRF
.WEB.SSRF · ADDRESSES ARE UTF-8 BYTE OFFSETS

AU: IDLE VIEW: POST VIEW