Image token counting SSRF protection can be bypassed via DNS rebinding

Low **ccurme** published **GHSA-r7w7-9xr2-qq2r** last week

Package

langchain-openai (pip)

Affected versions

<1.1.14

Patched versions

>=1.1.14

Description

Summary

`langchain-openai`'s `_url_to_size()` helper (used by `get_num_tokens_from_messages` for image token counting) validated URLs for SSRF protection and then fetched them in a separate network operation with independent DNS resolution. This left a TOCTOU / DNS rebinding window: an attacker-controlled hostname could resolve to a public IP during validation and then to a private/localhost IP during the actual fetch.

Severity: Low (CVSS:3.1 3.1)

The practical impact is limited because the fetched response body is passed directly to Pillow's `Image.open()` to extract dimensions — the response content is never returned, logged, or otherwise exposed to the caller. An attacker cannot exfiltrate data from internal services through this path. A potential risk is blind probing (inferring whether an internal host/port is open based on timing or error behavior).

Affected versions

- `langchain-openai` < 1.1.14

Patched versions

- `langchain-openai` >= 1.1.14 (requires `langchain-core` >= 1.2.31)

Affected code

File: `libs/partners/openai/langchain_openai/chat_models/base.py` — `_url_to_size()`

The vulnerable pattern was a validate-then-fetch with separate DNS resolution:

```
validate_safe_url(image_source, allow_private=False, allow_http=True)
# ... separate network operation with independent DNS resolution ...
response = httpx.get(image_source, timeout=timeout)
```

Fix

The fix replaces the validate-then-fetch pattern with an SSRF-safe httpx transport (`SSRFSafeSyncTransport` from `langchain-core`) that:

- Resolves DNS once and validates all returned IPs against a policy (private ranges, cloud metadata, localhost, k8s internal DNS)
- Pins the connection to the validated IP, eliminating the DNS rebinding window
- Disables redirect following to prevent redirect-based SSRF bypasses

This fix was released in langchain-openai 1.1.14.

Severity

Low 3.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

CVE ID

CVE-2026-41488

Weaknesses

▶ CWE-918

Credits

 **deprrous** Reporter