

f / prompts.chat Public

<> Code Issues 10 Pull requests 35 Actions Projects Models S

Commit 30a8f04



f committed 3 weeks ago · ✓ 4 / 4

fix(security): prevent SSRF & credential leakage via Fal.ai status polling

Add assertFalOrigin() validation to getFalRequestStatus and getFalRequestResult to ensure URLs point to trusted Fal.ai hosts (queue.fal.run, fal.run) before attaching the API key.

Ref: <https://gist.github.com/mdisec/27c0cac0ec6a8f3c8f85a18987ddb942>

main

1 parent [01f0587](#) commit 30a8f04

1 file changed +27 -0 lines changed

↑ Top ⚙️

Filter files...

src/lib/plugins/media-generators

fal.ts

1 file changed +27 -0 lines changed

Search within code ⚙️

src/lib/plugins/media-generators/fal.ts

```

@@ -24,6 +24,29 @@ import type {
24 24
25 25     const FAL_QUEUE_BASE = "https://queue.fal.run";
26 26
27 + const ALLOWED_FAL_HOSTS = new Set([
28 +   "queue.fal.run",
29 +   "fal.run",
30 +   ]);
31 +
32 + /**

```

```

33 + * Validate that a URL points to a trusted Fal.ai origin.
34 + *
35 + * Prevents SSRF by ensuring user-controlled tokens cannot redirect
36 + * authenticated requests to arbitrary servers.
37 + */
38 + export function assertFalOrigin(url: string): void {
39 +   let parsed: URL;
40 +   try {
41 +     parsed = new URL(url);
42 +   } catch {
43 +     throw new Error("Invalid Fal.ai URL");
44 +   }
45 +   if (parsed.protocol !== "https:" || !ALLOWED_FAL_HOSTS.has(parsed.hostname))
46 +     {
47 +       throw new Error("Invalid Fal.ai URL: untrusted origin");
48 +     }
49 + }

```

```

27 50   function parseModels(envVar: string | undefined, type: "image" | "video" |
    "audio"): MediaGeneratorModel[] {
28 51     if (!envVar) return [];
29 52     return envVar

```



```
@@ -112,6 +135,8 @@ async function submitToFalQueue(
```

```

112 135   export async function getFalRequestStatus(
113 136     statusUrl: string
114 137   ): Promise<FalStatusResponse> {

```

```

138 +   assertFalOrigin(statusUrl);
139 +

```

```

115 140     const apiKey = process.env.FAL_API_KEY;
116 141     if (!apiKey) throw new Error("FAL_API_KEY is not configured");
117 142

```



```
@@ -136,6 +161,8 @@ export async function getFalRequestStatus(
```

```

136 161   export async function getFalRequestResult(
137 162     responseUrl: string
138 163   ): Promise<FalImageOutput | FalVideoOutput | FalAudioOutput> {

```

```

164 +   assertFalOrigin(responseUrl);
165 +

```

```

139 166     const apiKey = process.env.FAL_API_KEY;
140 167     if (!apiKey) throw new Error("FAL_API_KEY is not configured");

```

141 168



Comments 0



Please [sign in](#) to comment.