Open Redirect via Shared Album name

Moderate **bo0tzz** published **GHSA-24fq-72x8-v7hm** yesterday

Package

immich-server (Docker)

Affected versions

< 2.7.3

Patched versions

>= 2.7.3

Description

Summary

An attacker (a registered user) can redirect the victim to any website (e.g. a modified version of Immich that collects login info), which helps massively with phishing attacks.

Details

An attacker creates a shared album with the name `0;url=https://attackersite.com" http-equiv="refresh`. They then create a share link for it, and give the link to the victim, who will get redirected to the attacker's site. The attack happens via the `<meta>` tag in api.service.ts:

immich/server/src/services/api.service.ts
Line 21 in `781d568`

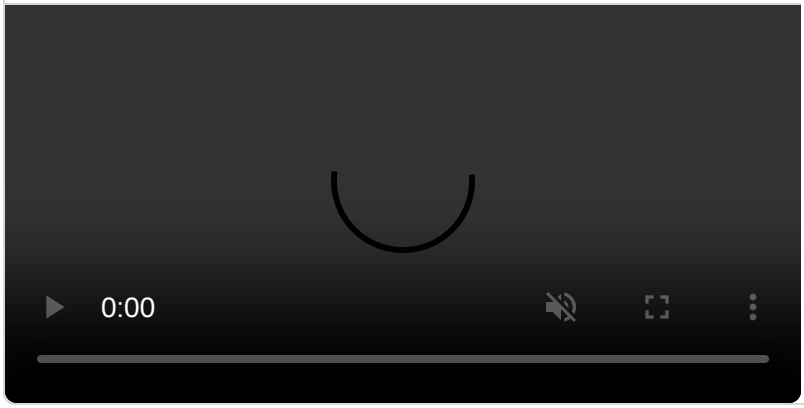
```
21          <meta property="og:title" content="${title}" />
```

I think the fix is to encode the value with HTML entities, so `"` would become `&quot;`. But I'm not 100% sure, there could be bypasses for that which I'm not aware of.

PoC

1. Create a new album
2. Give it the name `0;url=https://example.com" http-equiv="refresh`
3. Click on the Share icon, and copy the link
4. Open the link in a new browser tab
5. You should now get redirected to example.com

openredirect.mp4



Impact

This helps attackers a lot in phishing users. They could for example host a modified version of Immich at `https://immich.attacker.com` that asks for login when the victim opens it. The victim would think they need to log in to view the shared album, and the attacker would get the victim's login credentials to the original instance.

Severity

Moderate 5.1 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	Passive
Vulnerable System Impact Metrics	
Confidentiality	Low
Integrity	None
Availability	None
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

CVE ID

CVE-2026-40096

Weaknesses

- CWE-79
- CWE-601

Credits

Eldemarkki Reporter