Stored XSS via OCR Text in 360° Panorama Viewer

High **jrasm91** published **GHSA-9qx4-67jm-cc66** 2 days ago

Package

immich-server (Docker)

Affected versions	Patched versions
2.6.x	2.7.0

Description

Summary

Stored Cross-Site Scripting (XSS) in the 360° panorama viewer allows any authenticated user to execute arbitrary JavaScript in the browser of any other user who views the malicious panorama with the OCR overlay enabled. The attacker uploads an equirectangular image containing crafted text; OCR extracts it, and the panorama viewer renders it via `innerHTML` without sanitization. This enables session hijacking (via persistent API key creation), private photo exfiltration, and access to GPS location history and face biometric data.

Details

The `photo-sphere-viewer-adapter.svelte` component builds OCR tooltip content by interpolating `box.text` directly into an HTML template string, which is then passed to the `@photo-sphere-viewer` MarkersPlugin as `tooltip.content`. The MarkersPlugin renders this value via `innerHTML`.

Vulnerable code — `web/src/lib/components/asset-viewer/photo-sphere-viewer-adapter.svelte:141`:

```
const content = `<div class="${OCR_TOOLTIP_HTML_CLASS}" style="font-size: ${fontSi
```

`box.text` originates from the PaddleOCR pipeline, which stores raw model output without sanitization in `server/src/services/ocr.service.ts:84`:

```
text: rawText,
```

The regular (non-panorama) photo viewer is **not affected** — it uses Svelte's `{ocrBox.text}` template syntax (`ocr-bounding-box.svelte:63`), which auto-escapes HTML. Only the panorama code path bypasses this safe component and manually constructs HTML via template literal.

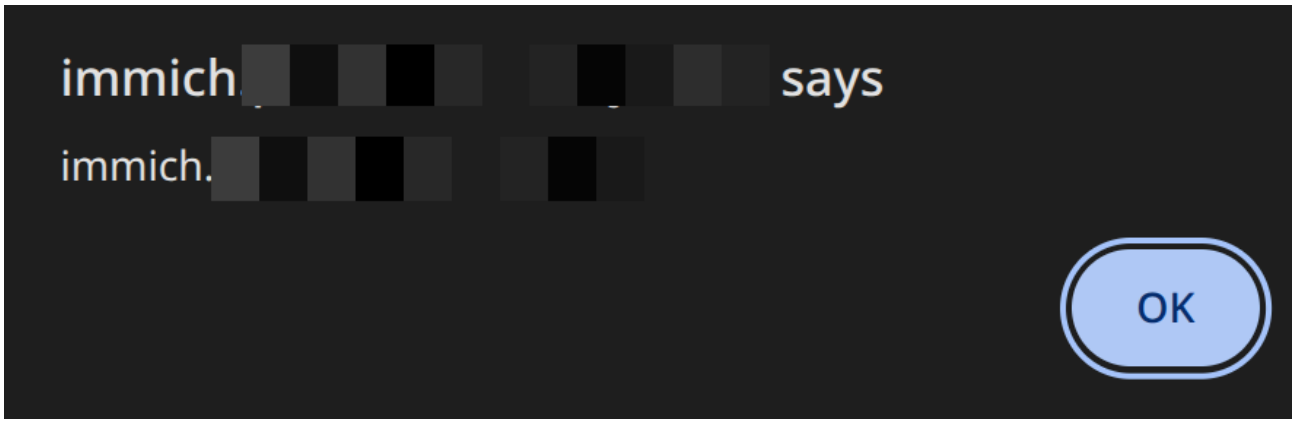
The application's Content Security Policy is disabled by default. When enabled via the bundled `helmet.json`, it includes `script-src 'unsafe-inline'`, which permits inline event handlers.

PoC

Prerequisites: An Immich instance with the default configuration (ML/OCR enabled, CSP disabled).

Upload this image:

Wait for the OCR to run, try to copy the password from the OCR. Watch the alert popup:



Impact

Any authenticated user who can upload images (default for all users) can attack any other user who views their panorama with the OCR overlay. Sharing a malicious panorama via a shared album is sufficient and then the victim clicking the OCR toggle and a detected text region.

Found by aisafe.io.

Severity

High 7.3 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2026-35455

Weaknesses

▶ CWE-79

Credits

Sijisu	Reporter
aisafe-bot	Finder