# WordPress Photo Engine Plugin <= 6.2.5 is vulnerable to Insecure Direct Object References (IDOR)

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2023-38513 |
| **State** | PUBLISHED |
| **Assigner** | Patchstack |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2023-12-20 14:15:19 UTC |
| **Updated** | 2026-04-28 19:21:03 UTC |
| **Description** | Authorization Bypass Through User-Controlled Key vulnerability in Jordy Meow Photo Engine (Media Organizer & Lightroo |

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-639 | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | nvd@nist.gov | Primary | 5.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N |
| 3.1 | audit@patchstack.com | Secondary | 5.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N |
| 3.1 | CNA | CVSS | 5.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Meowapps | Photo Engine | All | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Jordy Meow | Photo Engine Media Organizer Lightroom | affected n/a 6.2.5 custom | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| patchstack.com/database/vulnerability/wplr-sync/wordpress-photo-engine-plugi... | af854a3a-2127-422b-91ae-364da2661108 | patchstack.c |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Rafshanzani Suhada (Patchstack Alliance) (en)

## Additional Advisory Data

Solutions

**CNA:** Update to 6.2.6 or a higher version.

There are currently no legacy QID mappings associated with this CVE.

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**