



# Quick Playground <= 1.3.1 - Missing Authorization to Unauthenticated Arbitrary File Upload

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-1830
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-09 05:16:03 UTC
<b>Updated</b>	2026-04-24 18:03:42 UTC
<b>Description</b>	The Quick Playground plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.3.1.

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from security@wordfence.com

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

**EPSS:** 0.002350000 probability, percentile 0.463320000 (date 2026-04-27)

**Problem Types:** CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Davidfcarr	Quick Playground	affected 1.3.1 semver	Not specified

### References

Reference	Source	Link
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/quick-playground/trunk/expro-api.php	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/308cd28a-a477-4bc6-a392-ad5a9...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/quick-playground/trunk/api.php	security@wordfence.com	plugins.trac.wordpress.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

### Vendor Comments And Credit

Discovery Credit

**CNA:** Athiwat Tiprasaharn (en)

**CNA:** Itthidej Aramsri (en)

**CNA:** Vilaysone CHANTHAVONG (en)

**CNA:** Waris Damkham (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-02-03T23:23:04.000Z	Vendor Notified
CNA	2026-04-08T14:35:08.000Z	Disclosed

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

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)