



# WP Duplicate <= 1.1.8 - Authenticated (Subscriber+) Arbitrary File Upload via 'process\_add\_site' AJAX Action

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

## Summary

<b>CVE</b>	CVE-2026-1499
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-06 09:15:48 UTC
<b>Updated</b>	2026-04-08 17:21:10 UTC
<b>Description</b>	The WP Duplicate plugin for WordPress is vulnerable to Missing Authorization leading to Arbitrary File Upload in all version.

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from security@wordfence.com

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

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

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**High**

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Revmakx	WP Duplicate WordPress Migration Plugin	affected 1.1.8 semver	Not specified

### References

Reference	Source	Link
plugins.trac.wordpress.org/browser/local-sync/tags/1.1.8/includes/class-local-sync-handl...	security@wordfence.com	plugins.trac.wordpre
plugins.trac.wordpress.org/browser/local-sync/tags/1.1.8/admin/class-local-sync-files-op...	security@wordfence.com	plugins.trac.wordpre
www.wordfence.com/threat-intel/vulnerabilities/id/11bb7190-023b-45e1-99a5-7313c...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/local-sync/trunk/includes/class-local-sync-handle-ser...	security@wordfence.com	plugins.trac.wordpre
plugins.trac.wordpress.org/browser/local-sync/trunk/admin/class-local-sync-files-op.php	security@wordfence.com	plugins.trac.wordpre
plugins.trac.wordpress.org/browser/local-sync/trunk/admin/class-local-sync-admin.php	security@wordfence.com	plugins.trac.wordpre
plugins.trac.wordpress.org/browser/local-sync/tags/1.1.8/admin/class-local-sync-admin.php	security@wordfence.com	plugins.trac.wordpre
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpre
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)

### Additional Advisory Data

Source	Time	Event
CNA	2026-01-30T11:21:13.000Z	Vendor Notified
CNA	2026-02-05T19:59:16.000Z	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)