



# WordPress Shortcode Addons <= 3.2.5 - Arbitrary File Upload vulnerability

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

## Summary

<b>CVE</b>	CVE-2024-31114
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-03-31 18:15:47 UTC
<b>Updated</b>	2026-04-28 19:24:14 UTC
<b>Description</b>	Unrestricted Upload of File with Dangerous Type vulnerability in biplob018 Shortcode Addons.This issue affects Shortcode

## Risk And Classification

**Primary CVSS:** v3.1 9.1 CRITICAL from audit@patchstack.com

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

**EPSS:** 0.486600000 probability, percentile 0.977660000 (date 2026-04-28)

**Problem Types:** CWE-434 | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Biplob018	<a href="#">Shortcode Addons</a>	affected n/a 3.2.5 custom	Not specified
ADP	Oxilab	<a href="#">Shortcode Addons</a>	affected 3.2.5 custom	Not specified

### References

Reference	Source	Link
WordPress Shortcode Addons <= 3.2.5 - Arbitrary File Upload vulnerability - Patchstack	af854a3a-2127-422b-91ae-364da2661108	<a href="#">patches</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Peng Zhou (Patchstack Alliance) (en)

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)