



BackWPup <= 4.0.1 - Authenticated (Administrator+) Directory Traversal

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2023-5504
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-11 09:15:47 UTC
Updated	2026-04-08 19:18:49 UTC
Description	The BackWPup plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 4.0.1 via the Log

Risk And Classification

Primary CVSS: v3.1 8.7 HIGH from nvd@nist.gov

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

EPSS: 0.006490000 probability, percentile 0.708730000 (date 2026-05-06)

Problem Types: CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H
3.1	security@wordfence.com	Secondary	8.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H
3.1	CNA	DECLARED	8.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

High

Availability

High

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



NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Inpsyde	Backwpup	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wp Media	BackWPup WordPress Backup Restore Plugin	affected 4.0.1 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/backwpup/trunk/inc/class-page-settings.php	af854a3a-2127-422b-91ae-364da2661108	plugins.t
www.wordfence.com/threat-intel/vulnerabilities/id/e830fe1e-1171-46da-8ee7-0a665...	af854a3a-2127-422b-91ae-364da2661108	www.wo
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.t
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.



Vendor Comments And Credit

Discovery Credit

CNA: Marco Wotschka (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-10-10T00:00:00.000Z	Discovered
CNA	2023-11-22T00:00:00.000Z	Disclosed

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

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