



WordPress Core < 6.2.1 - Directory Traversal

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-2745
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-17 09:15:10 UTC
Updated	2026-04-08 19:18:19 UTC
Description	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

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	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordpress	Wordpress	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WordPress Foundation	WordPress	affected 4.1 4.1.38 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 4.2 4.2.35 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 4.3 4.3.31 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 4.4 4.4.30 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 4.5 4.5.29 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 4.6 4.6.26 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 4.7 4.7.26 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 4.8 4.8.22 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 4.9 4.9.23 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.0 5.0.19 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.1 5.1.16 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.2 5.2.18 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.3 5.3.15 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.4 5.4.13 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.5 5.5.12 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.6 5.6.11 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.7 5.7.9 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.8 5.8.7 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 5.9 5.9.6 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 6.0 6.0.4 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 6.1 6.1.2 semver	Not specified
CNA	WordPress Foundation	WordPress	affected 6.2 6.2.1 semver	Not specified

References

Reference	Source	Link
-----------	--------	------

WordPress Core < 6.2.1 - Directory Traversal	af854a3a-2127-422b-91ae-364da2661108	www.v
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	core.t
[SECURITY] [DLA 3462-1] wordpress security update	af854a3a-2127-422b-91ae-364da2661108	lists.d
www.exploit-db.com/exploits/52274	af854a3a-2127-422b-91ae-364da2661108	www.e
WordPress 6.2.1 Maintenance & Security Release – WordPress News	af854a3a-2127-422b-91ae-364da2661108	wordp
WordPress Core 6.2 XSS / CSRF / Directory Traversal ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108	packe
www.wordfence.com/blog/2023/05/wordpress-core-6-2-1-security-maintenance-releas...	security@wordfence.com	www.v
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

Vendor Comments And Credit

Discovery Credit

CNA: Ramuel Gall (en)

CNA: Matt Rusnak (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-05-16T00:00:00.000Z	Disclosed

Legacy QID Mappings

[154141](#) WordPress Directory Traversal Vulnerability (CVE-2023-2745)

[6000064](#) Debian Security Update for wordpress (DLA 3462-1)

[730803](#) WordPress Prior to 6.2.1 Multiple Vulnerabilities

© [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](#)