

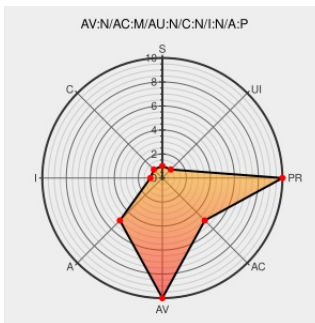


CVE-2009-3622

Published on: 10/23/2009 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:23 AM UTC

CVE-2009-3622

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Wordpress](#) from [Wordpress](#) contain the following vulnerability:

Algorithmic complexity vulnerability in wp-trackback.php in WordPress before 2.8.5 allows remote attackers to cause a denial of service (CPU consumption and server hang) via a long title parameter in conjunction with a charset parameter composed of many comma-separated "UTF-8" substrings, related to the mb_convert_encoding function in PHP.

CVE-2009-3622 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	Broken Link www.osvdb.org Inactive Link Not Archived	OSVDB 59077
403 Forbidden	Broken Link codes.zerial.org text/plain Inactive Link Not Archived	MISC codes.zerial.org/php/wp-trackbacks_dos.phps
Bug 530056 – CVE-2009-3622 WordPress: Resource exhaustion (DoS)	Issue Tracking bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=530056
WordPress › Blog › WordPress 2.8.5: Hardening Release	Vendor Advisory	CONFIRM

	wordpress.org text/html	wordpress.org/development/2009/10/wordpress-2-8-5-hardening-release/
Security-Shell: Wordpress Resource Exhaustion Denial of Service Exploit	Third Party Advisory security-sh3ll.blogspot.com text/html	MISC security-sh3ll.blogspot.com/2009/10/wordpress-resource-exhaustion-denial-of.html
No Description Provided	Exploit Issue Tracking Vendor Advisory rooibo.wordpress.com text/html	MISC rooibo.wordpress.com/2009/10/17/agujero-de-seguridad-en-wordpress/
Full Disclosure: [Wordpress] Resource Exhaustion (Denial of Service)	Exploit Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20091019 [Wordpress] Resource Exhaustion (Denial of Service)
WordPress Trackback Denial of Service Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 37088
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	XF wordpress-wptrackback-dos(53884)
'[oss-security] CVE request: Wordpress Trackback DoS' - MARC	Mailing List Third Party Advisory marc.info text/html	MLIST [oss-security] 20091021 CVE request: Wordpress Trackback DoS
SecurityTracker.com Archives - WordPress 'wp-trackbacks.php' Multi-byte Encoding Detection Lets Remote Users Execute Arbitrary Code	Third Party Advisory VDB Entry securitytracker.com text/html	SECTRAK 1023072
'Re: [oss-security] CVE request: Wordpress Trackback DoS' - MARC	Mailing List Third Party Advisory marc.info text/html	MLIST [oss-security] 20091021 Re: CVE request: Wordpress Trackback DoS
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Patch Vendor Advisory www.vupen.com text/html	VUPEN ADV-2009-2986

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordpress	Wordpress	All	All	All	All
cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023   |

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](#).

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