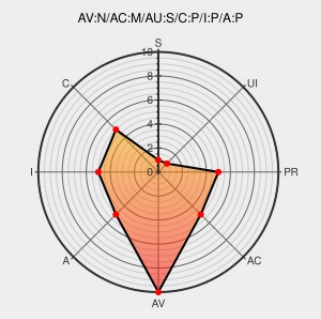
CVE-2009-3890

Published on: 11/17/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:24 PM UTC

CVE-2009-3890

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wordpress from Wordpress contain the following vulnerability:

Unrestricted file upload vulnerability in the wp_check_filetype function in wp-includes/functions.php in WordPress before 2.8.6, when a certain configuration of the mod_mime module in the Apache HTTP Server is enabled, allows remote authenticated users to execute arbitrary code by posting an attachment with a multiple-extension filename, and then accessing this attachment via a direct request to a wp-content/uploads/ pathname, as demonstrated by a .php.jpg filename.

CVE-2009-3890 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
NEOHAPSIS - Peace of Mind Through Integrity and Insight	Broken Link, web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20091112 Re: WordPress <= 2.8.5 Unrestricted File Upload Arbitrary PHP Code Execution
No Description Provided	Broken Link, www.osvdb.org, Inactive Link, Not Archived	OSVDB 59958
oss-security - Re: CVE request: Wordpress 2.8.6	Mailing List, Third Party Advisory	MLIST [oss-security] 20091115 Re: CVE request: Wordpress 2.8.6

	www.openwall.com text/html	
NEOHAPSIS - Peace of Mind Through Integrity and Insight	Broken Link web.archive.org text/html Inactive Link Not Archived	FULLDISC 20091111 WordPress <= 2.8.5 Unrestricted File Upload Arbitrary PHP Code Execution
NEOHAPSIS - Peace of Mind Through Integrity and Insight	Broken Link web.archive.org text/html Inactive Link Not Archived	FULLDISC 20091112 Re: WordPress <= 2.8.5 Unrestricted File Upload Arbitrary PHP Code Execution
oss-security - Re: CVE request: Wordpress 2.8.6	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20091116 Re: CVE request: Wordpress 2.8.6
WordPress › Blog » WordPress 2.8.6 Security Release	Patch Vendor Advisory wordpress.org text/html	CONFIRM wordpress.org/development/2009/11/wordpress-2-8-6-security-release/
WordPress File Upload and Script Insertion - Secunia Advisories - Vulnerability Information - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 37332
oss-security - CVE request: Wordpress 2.8.6	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20091115 CVE request: Wordpress 2.8.6
#11122 (Sanitize filenames with multiple extensions) – WordPress Trac	Issue Tracking Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM core.trac.wordpress.org/ticket/11122

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 and Source URL Uptime Status status.cve.report