



CVE-2007-2024

Published on: 04/13/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:42 PM UTC

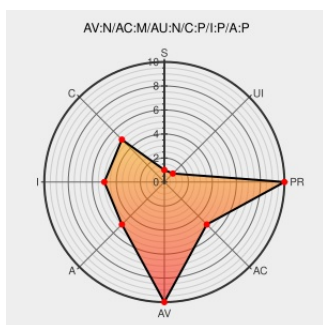
CVE-2007-2024

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Unrestricted file upload vulnerability in the UpLoad feature (lib/plugin/UpLoad.php) in PhpWiki 1.3.x allows remote attackers to upload arbitrary PHP files with a (1) php3, (2) php4, or (3) php5 extension.

CVE-2007-2024 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Debian update for phpwiki - Advisories - Secunia

[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 26784](#)

SecurityFocus

[www.securityfocus.com](#)
[text/html](#)

[BUGTRAQ 20070412 RE: Critical phpwiki c99shell exploit](#)

US-CERT Vulnerability Note VU#914793

[US Government Resource](#)
[www.kb.cert.org](#)
[text/html](#)

[CERT-VN VU#914793](#)

Gentoo Linux Documentation -- PhpWiki: Remote execution of arbitrary code

[www.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-200705-16](#)

Nabble - Fwd: Critical phpwiki c99shell exploit

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[MLIST \[phpwiki-talk\] 20070413 Fwd: Critical phpwiki c99shell exploit](#)

Gentoo update for PhpWiki - Advisories - Secunia	web.archive.org text/html	 SECUNIA 25307
PhpWiki "UpLoad" PHP Script Upload Vulnerability - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 24888
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20070412 Re: Critical phpwiki c99shell exploit
Debian -- Security Information -- DSA-1371-1 phpwiki	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1371
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2007-1400
SecurityFocus	web.archive.org text/html Inactive Link Not Archived	 BUGTRAQ 20070412 Critical phpwiki c99shell exploit

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	Phpwiki	Phpwiki	1.3.x	All	All	All
Application	Phpwiki	Phpwiki	1.3.x	All	All	All
<code>cpe:2.3:a:phpwiki:phpwiki:1.3.x:****:****:*</code>						
<code>cpe:2.3:a:phpwiki:phpwiki:1.3.x:****:****:*</code>						

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](#)