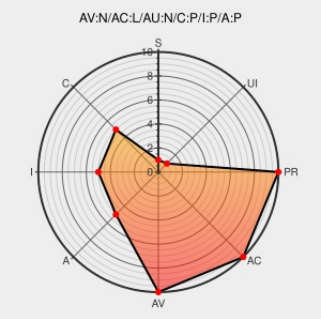
CVE-2005-1921

Published on: 07/01/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:25 AM UTC

CVE-2005-1921

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



Certain versions of Xml Rpc from Pear contain the following vulnerability:

Eval injection vulnerability in PEAR XML_RPC 1.3.0 and earlier (aka XML-RPC or xmlrpc) and PHPXMLRPC (aka XML-RPC For PHP or php-xmlrpc) 1.1 and earlier, as used in products such as (1) WordPress, (2) Serendipity, (3) Drupal, (4) egroupware, (5) MailWatch, (6) TikiWiki, (7) phpWebSite, (8) Ampache, and others, allows remote attackers to execute arbitrary PHP code via an XML file, which is not properly sanitized before being used in an eval statement.

CVE-2005-1921 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
XML-RPC for PHP Remote Code Injection Vulnerability	cve.report (archive) text/html	BID 14088
Secunia - Advisories - XOOPS PHPMailer and XML-RPC Vulnerabilities	web.archive.org text/html	SECUNIA 16339
Page not found - SourceForge.net	sourceforge.net text/html Inactive Link Not Archived	CONFIRM sourceforge.net/project/shownotes.php?release_id=338803
Secunia - Advisories - Ampache XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15957

Secunia - Advisories - TikiWiki XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15944
Hardened-PHP Project - PHP Security - Advisory 02/2005	Vendor Advisory www.hardened-php.net text/html	MISC www.hardened-php.net/advisory-022005.php
Gentoo Linux Documentation -- TikiWiki: Arbitrary command execution through XML-RPC	security.gentoo.org text/html	GENTOO GLSA-200507-06
Security advisories | Drupal.org	www.drupal.org text/html	CONFIRM www.drupal.org/security/drupal-sa-2005-003/advisory.txt
Secunia - Advisories - b2evolution XML-RPC PHP Code Execution Vulnerabilities	web.archive.org text/html	SECUNIA 17440
Secunia - Advisories - PostNuke XML-RPC Library PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15855
Secunia - Advisories - Jaws "path" File Inclusion and XML-RPC PHP Code Execution	web.archive.org text/html	SECUNIA 15922
Debian -- Security Information -- DSA-747-1 egroupware	www.debian.org Depreciated Link text/html	DEBIAN DSA-747
Secunia - Advisories - phpPgAds XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15884
Secunia - Advisories - MAXdev MD-Pro Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 16693
Debian -- Security Information -- DSA-789-1 php4	www.debian.org Depreciated Link text/html	DEBIAN DSA-789
[A] m p a c h e : For the love of music since May 5th 2001	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.ampache.org/announce/3_3_1_2.php
SourceForge.net: Project Filelist	sourceforge.net text/html	CONFIRM sourceforge.net/project/showfiles.php?group_id=87163
Secunia - Advisories - PhpWiki XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15903
Debian -- Security Information -- DSA-745-1 drupal	www.debian.org Depreciated Link text/html	DEBIAN DSA-745
'Advisory 02/2005: Remote code execution in Serendipity' - MARC	marc.info text/html	BUGTRAQ 20050629 Advisory 02/2005: Remote code execution in Serendipity
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2827
Debian -- Security Information -- DSA-746-1 phpgroupware	www.debian.org Depreciated Link text/html	DEBIAN DSA-746
Secunia - Advisories - Nucleus XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15895
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2005:049

Secunia - Advisories - BLOG:CMS XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15904
Secunia - Advisories - phpAdsNew XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15883
Secunia - Advisories - phpGroupWare XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15917
Gentoo Linux Documentation -- PEAR XML-RPC, phpxmlrpc: PHP script injection vulnerability	security.gentoo.org text/html	GENTOO GLSA-200507-01
Secunia - Advisories - XML-RPC for PHP PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15852
Secunia - Advisories - MailWatch for MailScanner XML-RPC PHP Code Execution	web.archive.org text/html	SECUNIA 15947
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:350
Advisories - Mandriva	Patch Vendor Advisory www.mandriva.com text/html	MANDRAKE MDKSA-2005:109
Gentoo Linux Documentation -- phpWebSite: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-200507-07
'[DRUPAL-SA-2005-003] Drupal 4.6.2 / 4.5.4 fixes critical XML-RPC issue' - MARC	marc.info text/html	BUGTRAQ 20050629 [DRUPAL-SA-2005-003] Drupal 4.6.2 / 4.5.4 fixes critical XML-RPC issue
FreeMED XML_RPC PHP Code Execution Vulnerability - Advisories - Secunia	web.archive.org text/html	SECUNIA 17674
Secunia - Advisories - PEAR XML_RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15861
Contact Support	Patch Vendor Advisory www.gulftech.org text/html	MISC www.gulftech.org/?node=research&article_id=00087-07012005
Secunia - Advisories - eGroupWare XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15916
SecurityTracker.com Archives - HP Secure Web Server for Tru64 UNIX XMLRPC Bug Lets Remote Users Execute Arbitrary PHP Code	securitytracker.com text/html	SECTRACK 1015336
Secunia - Advisories - phpMyFAQ XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 15810
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2005:018
Secunia - Advisories - Drupal PHP Code Execution Vulnerabilities	web.archive.org text/html	SECUNIA 15872
'SUSE Security Announcement: php4, php5 remote code execution' - MARC	marc.info text/html	SUSE SUSE-SA:2005:051
SecurityFocus	www.securityfocus.com text/html	HP SSRT051069
Secunia - Advisories - phpWebSite PEAR XML_RPC PHP	web.archive.org	SECUNIA 16001

Code Execution	text/html	
PEAR :: Package :: XML_RPC :: 1.3.1	Patch pear.php.net text/xml	MISC pear.php.net/package/XML_RPC/download/1.3.1
Secunia - Advisories - HP Tru64 UNIX Secure Web Server XML_RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 18003
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:564
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2005:041
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11294

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	Pear	Xml Rpc	1.0.2	All	All	All
Application	Pear	Xml Rpc	1.0.3	All	All	All
Application	Pear	Xml Rpc	1.0.4	All	All	All
Application	Pear	Xml Rpc	1.1.0	All	All	All
Application	Pear	Xml Rpc	1.2.0	All	All	All
Application	Pear	Xml Rpc	1.2.0rc1	All	All	All
Application	Pear	Xml Rpc	1.2.0rc2	All	All	All
Application	Pear	Xml Rpc	1.2.0rc3	All	All	All
Application	Pear	Xml Rpc	1.2.0rc4	All	All	All
Application	Pear	Xml Rpc	1.2.0rc5	All	All	All
Application	Pear	Xml Rpc	1.2.0rc6	All	All	All
Application	Pear	Xml Rpc	1.2.0rc7	All	All	All
Application	Pear	Xml Rpc	1.2.1	All	All	All
Application	Pear	Xml Rpc	1.2.2	All	All	All
Application	Pear	Xml Rpc	1.3.0rc1	All	All	All
Application	Pear	Xml Rpc	1.3.0rc2	All	All	All
Application	Pear	Xml Rpc	1.3.0rc3	All	All	All
Application	Pear	Xml Rpc	1.0.2	All	All	All

Application	Pear	Xml Rpc	1.0.3	All	All	All
Application	Pear	Xml Rpc	1.0.4	All	All	All
Application	Pear	Xml Rpc	1.1.0	All	All	All
Application	Pear	Xml Rpc	1.2.0	All	All	All
Application	Pear	Xml Rpc	1.2.0rc1	All	All	All
Application	Pear	Xml Rpc	1.2.0rc2	All	All	All
Application	Pear	Xml Rpc	1.2.0rc3	All	All	All
Application	Pear	Xml Rpc	1.2.0rc4	All	All	All
Application	Pear	Xml Rpc	1.2.0rc5	All	All	All
Application	Pear	Xml Rpc	1.2.0rc6	All	All	All
Application	Pear	Xml Rpc	1.2.0rc7	All	All	All
Application	Pear	Xml Rpc	1.2.1	All	All	All
Application	Pear	Xml Rpc	1.2.2	All	All	All
Application	Pear	Xml Rpc	1.3.0rc1	All	All	All
Application	Pear	Xml Rpc	1.3.0rc2	All	All	All
Application	Pear	Xml Rpc	1.3.0rc3	All	All	All

cpe:2.3:a:pear:xml_rpc:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc1:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc2:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc3:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc4:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc5:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc6:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc7:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.3.0rc1:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.3.0rc2:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.3.0rc3:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc1:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc2:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc3:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc4:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc5:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc6:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.0rc7:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.3.0rc1:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.3.0rc2:*:*:*:*:*:*:*:

cpe:2.3:a:pear:xml_rpc:1.3.0rc3:*:*:*:*:*:*:*:

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 registred 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