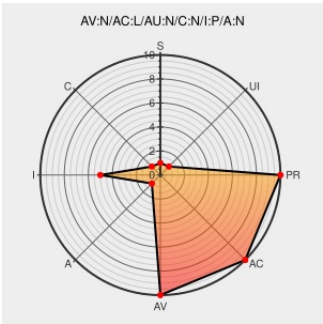
CVE-2005-2498

Published on: 08/15/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:26 AM UTC

CVE-2005-2498

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



Certain versions of Phpxmlrpc from Edd Dumbill contain the following vulnerability:

Eval injection vulnerability in PHPXMLRPC 1.1.1 and earlier (PEAR XML-RPC for PHP), as used in multiple products including (1) Drupal, (2) phpAdsNew, (3) phpPgAds, and (4) phpgroupware, allows remote attackers to execute arbitrary PHP code via certain nested XML tags in a PHP document that should not be nested, which are injected into an eval function call, a different vulnerability than CVE-2005-1921.

CVE-2005-2498 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Secunia - Advisories - SUSE update for php4/php5	web.archive.org text/html	SECUNIA 16619
Secunia - Advisories - Debian update for egroupware	web.archive.org text/html	SECUNIA 17066
Secunia - Advisories - phpGroupWare Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 16558
Secunia - Advisories - phpPgAds Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 16469
Secunia - Advisories - b2evolution XML-RPC PHP Code Execution Vulnerabilities	web.archive.org text/html	SECUNIA 17440

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
Secunia - Advisories - phpAdsNew Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 16468
PHPXMLRPC and PEAR XML_RPC Remote Code Injection Vulnerability	cve.report (archive) text/html	BID 14560
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9569
Debian -- Security Information -- DSA-798-1 phpgroupware	www.debian.org Depreciated Link text/html	DEBIAN DSA-798
Secunia - Advisories - Drupal XML-RPC PHP Code Execution Vulnerability	web.archive.org text/html	SECUNIA 16432
Secunia - Advisories - Nucleus CMS XML-RPC Nested XML Tags PHP Code Execution	web.archive.org text/html	SECUNIA 16460
Secunia - Advisories - eGroupWare XML-RPC Nested XML Tags PHP Code Execution	web.archive.org text/html	SECUNIA 16465
Debian -- Security Information -- DSA-842-1 egroupware	www.debian.org Depreciated Link text/html	DEBIAN DSA-842
Hardened-PHP Project - PHP Security - Advisory 15/2005	Patch Vendor Advisory www.hardened-php.net text/html	MISC www.hardened-php.net/advisory_152005.67.html
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2005:049
Secunia - Advisories - phpMyFAQ XML-RPC Nested XML Tags PHP Code Execution	web.archive.org text/html	SECUNIA 16441
The Fedora Legacy Project	web.archive.org text/html Inactive Link Not Archived	FEDORA FLSA:166943
Debian -- Security Information -- DSA-840-1 drupal	www.debian.org Depreciated Link text/html	DEBIAN DSA-840
Secunia - Advisories - TikiWiki XML-RPC Nested XML Tags PHP Code Execution	web.archive.org text/html	SECUNIA 16563
Secunia - Advisories - Gentoo update for php	web.archive.org text/html	SECUNIA 16976
'[PHPADSNEW-SA-2005-001] phpAdsNew and phpPgAds 2.0.6 fix multiple' - MARC	marc.info text/html	BUGTRAQ 20050817 [PHPADSNEW-SA-2005-001] phpAdsNew and phpPgAds 2.0.6 fix multiple vulnerabilities
Secunia - Advisories - MailWatch for MailScanner XML-RPC PHP Code Execution	web.archive.org text/html	SECUNIA 16491
Secunia - Advisories - Gentoo update for PEAR-	web.archive.org	SECUNIA 16550

XML_RPC / phpxmlrpc	text/html	
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20050815 Advisory 15/2005: PHPXMLRPC Remote PHP Code Injection Vulnerability
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:748
Gentoo Linux Documentation -- PHP: Vulnerabilities in included PCRE and XML-RPC libraries	www.gentoo.org text/html	GENTOO GLSA-200509-19
Secunia - Advisories - XML-RPC for PHP Nested XML Tags PHP Code Execution	web.archive.org text/html	SECUNIA 16431
'SUSE Security Announcement: php4, php5 remote code execution' - MARC	marc.info text/html	SUSE SUSE-SA:2005:051
Secunia - Advisories - Slackware update for php	web.archive.org text/html	SECUNIA 16635
Secunia - Advisories - Debian update for drupal	web.archive.org text/html	SECUNIA 17053
'[DRUPAL-SA-2005-004] Drupal 4.6.3 / 4.5.5 fixes critical XML-RPC issue' - MARC	marc.info text/html	BUGTRAQ 20050815 [DRUPAL-SA-2005-004] Drupal 4.6.3 / 4.5.5 fixes critical XML-RPC issue

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Edd Dumbill	Phpxmlrpc	1.1.1	All	All	All
Application	Edd Dumbill	Phpxmlrpc	1.1.1	All	All	All

cpe:2.3:a:edd_dumbill:phpxmlrpc:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:edd_dumbill:phpxmlrpc:1.1.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report