

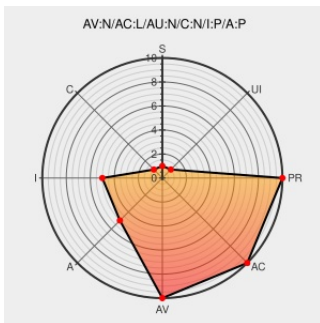


CVE-2008-3659

Published on: 08/14/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:12 PM UTC

CVE-2008-3659

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

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

Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.

CVE-2008-3659 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

'[security bulletin] HPSBUX02465
SSRT090192 rev.1 - HP-UX Running
Apache-based Web Server, Remote Den'
- MARC

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[HP HPSBUX02465](#)

oss-security - CVE request: php-5.2.6
overflow issues

[www.openwall.com](#)

[text/html](#)

[MLIST \[oss-security\] 20080808 CVE request: php-5.2.6
overflow issues](#)

[security-announce] SUSE Security
Summary Report: SUSE-SR:2008:018

[lists.opensuse.org](#)

[text/html](#)

[SUSE SUSE-SR:2008:018](#)

php.cvs: cvs: php-src(PHP_5_2)
/ext/standard/tests/strings
explode_bug.phpt ZendEngine2
zend_operators.h

[news.php.net](#)

[text/x-diff](#)

[CONFIRM news.php.net/php.cvs/52002](#)

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF php-memnstr-bo(44405)
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:021	lists.opensuse.org text/html	 SUSE SUSE-SR:2008:021
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 32316
PHP: News Archive - 2008	Patch www.php.net text/html	 CONFIRM www.php.net/archive/2008.php#id2008-08-07-1
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 31982
Gentoo Bug 234102 - dev-lang/php < 5.2.6-r6: arbitrary code execution, DoS, safe_mode bypass (CVE-2008-{3658,3659,3660})	bugs.gentoo.org text/html	 CONFIRM bugs.gentoo.org/show_bug.cgi?id=234102
Support / Security / Advisories // MDVSA-2009:024 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2009:024
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 35074
About Secunia Research Flexera	web.archive.org text/html	 SECUNIA 32148
SecurityTracker.com Archives - PHP Buffer Overflow in explode() Function May Let Users Bypass Safe Mode Restrictions	www.securitytracker.com text/html	 SECTrack 1020995
About the security content of Security Update 2009-002 / Mac OS X v10.5.7	support.apple.com text/html	 CONFIRM support.apple.com/kb/HT3549
US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/xml	 CERT TA09-133A
Debian -- Security Information -- DSA-1647-1 php5	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1647
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2009-1297
Gentoo update for php - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 32746
No Description Provided	osvdb.org Inactive Link Not Archived	 OSVDB 47483
Advisories Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2009:021
Advisories Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2009:022

	text/html	
Advisories:rPSA-2009-0035 - rPath Wiki	web.archive.org text/html Inactive Link Not Archived	 CONFIRM wiki.rpath.com/Advisories:rPSA-2009-0035
APPLE-SA-2009-05-12 Security Update 2009-002 / Mac OS X v10.5.7	lists.apple.com text/html	 APPLE APPLE-SA-2009-05-12
Advisories Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2009:023
HP-UX Apache Web Server Suite Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 35650
oss-security - Re: CVE request: php-5.2.6 overflow issues	www.openwall.com text/html	 MLIST [oss-security] 20080813 Re: CVE request: php-5.2.6 overflow issues
oss-security - Re: CVE request: php-5.2.6 overflow issues	www.openwall.com text/html	 MLIST [oss-security] 20080808 Re: CVE request: php-5.2.6 overflow issues
No Description Provided	web.archive.org text/html Inactive Link Not Archived	 HP SSRT090085
PHP: Multiple vulnerabilities — Gentoo Linux Documentation	security.gentoo.org text/html	 GENTOO GLSA-200811-05
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2008-2336
oss-security - Re: CVE request: php-5.2.6 overflow issues	www.openwall.com text/html	 MLIST [oss-security] 20080808 Re: CVE request: php-5.2.6 overflow issues

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	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	4.4.3	All	All	All
Application	Php	Php	4.4.4	All	All	All
Application	Php	Php	4.4.5	All	All	All
Application	Php	Php	4.4.6	All	All	All
Application	Php	Php	4.4.7	All	All	All
Application	Php	Php	4.4.8	All	All	All
Application	Php	Php	5.2.0	All	All	All

Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
Application	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All
Application	Php	Php	4.4.3	All	All	All
Application	Php	Php	4.4.4	All	All	All
Application	Php	Php	4.4.5	All	All	All
Application	Php	Php	4.4.6	All	All	All
Application	Php	Php	4.4.7	All	All	All
Application	Php	Php	4.4.8	All	All	All
Application	Php	Php	5.2.0	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	5.2.2	All	All	All
Application	Php	Php	5.2.3	All	All	All
Application	Php	Php	5.2.4	All	All	All
Application	Php	Php	5.2.5	All	All	All
Application	Php	Php	5.2.6	All	All	All
cpe:2.3:a:php:php:4.4.0:*****:						
cpe:2.3:a:php:php:4.4.1:*****:						
cpe:2.3:a:php:php:4.4.2:*****:						
cpe:2.3:a:php:php:4.4.3:*****:						
cpe:2.3:a:php:php:4.4.4:*****:						
cpe:2.3:a:php:php:4.4.5:*****:						
cpe:2.3:a:php:php:4.4.6:*****:						
cpe:2.3:a:php:php:4.4.7:*****:						
cpe:2.3:a:php:php:4.4.8:*****:						
cpe:2.3:a:php:php:5.2.0:*****:						
cpe:2.3:a:php:php:5.2.1:*****:						

cpe:2.3:a:php:php:5.2.2:*****:
cpe:2.3:a:php:php:5.2.3:*****:
cpe:2.3:a:php:php:5.2.4:*****:
cpe:2.3:a:php:php:5.2.5:*****:
cpe:2.3:a:php:php:5.2.6:*****:
cpe:2.3:a:php:php:4.4.0:*****:
cpe:2.3:a:php:php:4.4.1:*****:
cpe:2.3:a:php:php:4.4.2:*****:
cpe:2.3:a:php:php:4.4.3:*****:
cpe:2.3:a:php:php:4.4.4:*****:
cpe:2.3:a:php:php:4.4.5:*****:
cpe:2.3:a:php:php:4.4.6:*****:
cpe:2.3:a:php:php:4.4.7:*****:
cpe:2.3:a:php:php:4.4.8:*****:
cpe:2.3:a:php:php:5.2.0:*****:
cpe:2.3:a:php:php:5.2.1:*****:
cpe:2.3:a:php:php:5.2.2:*****:
cpe:2.3:a:php:php:5.2.3:*****:
cpe:2.3:a:php:php:5.2.4:*****:
cpe:2.3:a:php:php:5.2.5:*****:
cpe:2.3:a:php:php:5.2.6:*****:

[← 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](#)