



CVE-2007-3996

Published on: 09/04/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:34 PM UTC

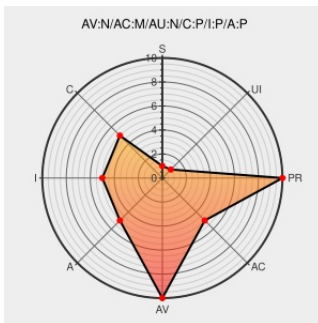
CVE-2007-3996

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Multiple integer overflows in libgd in PHP before 5.2.4 allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a large (1) srcW or (2) srcH value to the (a) gdImageCopyResized function, or a large (3) sy (height) or (4) sx (width) value to the (b) gdImageCreate or the (c) gdImageCreateTrueColor function.

CVE-2007-3996 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF php-gdimagecreate-bo(36382)
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2007-3023
	www.trustix.org text/plain Inactive Link Not Archived	TRUSTIX 2007-0026
PHP ImageCreate/ImageCreateTrueColor Integer Overflow	web.archive.org text/html Inactive Link Not Archived	MISC secweb.se/en/advisories/php-imagecreatetruecolor-integer-overflow/
Avaya Products PHP Multiple Vulnerabilities - Advisories -	web.archive.org	SECUNIA 27545

Secunia	text/html	
Ubuntu update for libgd2 - Advisories - Secunia	web.archive.org text/html	 SECUNIA 28147
Gentoo Linux Documentation -- E2fsprogs: Multiple buffer overflows	security.gentoo.org text/html	 GENTOO GLSA-200712-13
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:11147
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2007:0888
Fedora update for php - Advisories - Secunia	web.archive.org text/html	 SECUNIA 26930
Red Hat update for php - Advisories - Secunia	web.archive.org text/html	 SECUNIA 26871
SecurityReason - PHP ImageCopyResized/ImageCopyResampled Integer Overflow	securityreason.com text/html	 SREASON 3103
rPath Update for Multiple php Packages - Advisories - Secunia	web.archive.org text/html	 SECUNIA 26838
USN-557-1: GD library vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-557-1
PHP: PHP 5.2.4 Release Announcement	www.php.net text/html	 CONFIRM www.php.net/releases/5_2_4.php
PHP ImageCopyResized/ImageCopyResampled Integer Overflow	Patch web.archive.org text/html Inactive Link Not Archived	 MISC secweb.se/en/advisories/php-imagecopyresized-integer-overflow/
Red Hat update for php - Advisories - Secunia	web.archive.org text/html	 SECUNIA 27351
No Description Provided	issues.rpath.com Inactive Link Not Archived	 CONFIRM issues.rpath.com/browse/RPL-1702
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2007:0890
Gentoo Linux Documentation -- PHP: Multiple vulnerabilities	www.gentoo.org text/html	 GENTOO GLSA-200710-02
No Description Provided	issues.rpath.com Inactive Link Not Archived	 CONFIRM issues.rpath.com/browse/RPL-1693
Gentoo update for e2fsprogs - Advisories - Secunia	web.archive.org text/html	 SECUNIA 28009
[security-announce] SUSE Security Announcement: php4, php5 (SUSE-SA:2008)	lists.opensuse.org text/html	 SUSE SUSE-SA:2008:004
ASA-2007-449 (RHSA-2007-0888, RHSA-2007-0889 & RHSA-2007-0890)	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2007-449.htm
SUSE update for php4 and php5 - Advisories - Secunia	web.archive.org text/html	 SECUNIA 28658
Gentoo Bug 201546 - sys-fs/e2fsprogs < 1.40.3 Multiple buffer overflows (CVE-2007-5497)	bugs.gentoo.org text/html	 CONFIRM bugs.gentoo.org/show_bug.cgi?id=201546

Gentoo update for php - Advisories - Secunia	web.archive.org text/html	 SECUNIA 27102
Debian update for libgd2 - Advisories - Secunia	web.archive.org text/html	 SECUNIA 31168
rPath update for php, php-mysql and php-pgsql - Advisories - Secunia	web.archive.org text/html	 SECUNIA 27377
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2007:0891
Mandriva update for php - Advisories - Secunia	web.archive.org text/html	 SECUNIA 26895
PHP: PHP 5 ChangeLog	Patch www.php.net text/html	 CONFIRM www.php.net/ChangeLog-5.php#5.2.4
Trustix Update for Multiple Packages - Advisories - Secunia	web.archive.org text/html	 SECUNIA 26822
Red Hat update for php - Advisories - Secunia	web.archive.org text/html	 SECUNIA 26967
rhn.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2007:0889
[SECURITY] Fedora Core 6 Update: php-5.1.6-3.7.fc6	www.redhat.com text/html	 FEDORA FEDORA-2007-709
Debian -- Security Information -- DSA-1613-1 libgd2	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1613
Advisories Mandriva	www.mandriva.com text/html	 MANDRIVA MDKSA-2007:187
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF php-gdimagecopyresized-bo(36383)
PHP Multiple Vulnerabilities - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 26642

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	All	All	All	All
cpe:2.3:a:php:php:*****:						

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](#)