



# CVE-2007-1001

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2007-1001                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                        |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2007-04-06 00:19:00 UTC                                                                                                    |
| <b>Updated</b>         | 2018-10-30 16:25:00 UTC                                                                                                    |
| <b>Description</b>     | Multiple integer overflows in the (1) createwbmp and (2) readwbmp functions in wbmp.c in the GD library (libgd) in PHP 4.0 |

## Risk And Classification

### Problem Types: CWE-189

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor              | Product             | Version | Update        | Edition | Language |
|-------------|---------------------|---------------------|---------|---------------|---------|----------|
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0     | All           | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0     | beta1         | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0     | beta2         | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0     | beta3         | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0     | beta4         | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0     | beta_4_patch1 | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0     | rc1           | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0     | rc2           | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.0   | All           | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.1   | All           | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.1   | patch1        | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.1   | patch2        | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.2   | All           | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.3   | All           | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.3   | patch1        | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.4   | All           | All     | All      |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 4.0.4   | patch1        | All     | All      |

|             |     |     |        |     |     |     |
|-------------|-----|-----|--------|-----|-----|-----|
|             |     |     |        |     |     |     |
| Application | Php | Php | 4.0.5  | All | All | All |
| Application | Php | Php | 4.0.6  | All | All | All |
| Application | Php | Php | 4.0.7  | All | All | All |
| Application | Php | Php | 4.0.7  | rc1 | All | All |
| Application | Php | Php | 4.0.7  | rc2 | All | All |
| Application | Php | Php | 4.0.7  | rc3 | All | All |
| Application | Php | Php | 4.1.0  | All | All | All |
| Application | Php | Php | 4.1.1  | All | All | All |
| Application | Php | Php | 4.1.2  | All | All | All |
| Application | Php | Php | 4.2    | All | dev | All |
| Application | Php | Php | 4.2.0  | All | All | All |
| Application | Php | Php | 4.2.1  | All | All | All |
| Application | Php | Php | 4.2.2  | All | All | All |
| Application | Php | Php | 4.2.3  | All | All | All |
| Application | Php | Php | 4.3.0  | All | All | All |
| Application | Php | Php | 4.3.1  | All | All | All |
| Application | Php | Php | 4.3.10 | All | All | All |
| Application | Php | Php | 4.3.11 | All | All | All |
| Application | Php | Php | 4.3.2  | All | All | All |
| Application | Php | Php | 4.3.3  | All | All | All |
| Application | Php | Php | 4.3.4  | All | All | All |
| Application | Php | Php | 4.3.5  | All | All | All |
| Application | Php | Php | 4.3.6  | All | All | All |
| Application | Php | Php | 4.3.7  | All | All | All |
| Application | Php | Php | 4.3.8  | All | All | All |
| Application | Php | Php | 4.3.9  | 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 | 5.0    | rc1 | All | All |
| Application | Php | Php | 5.0    | rc2 | All | All |

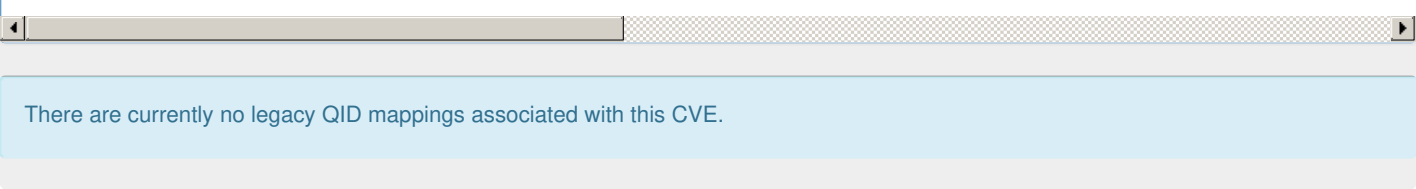
|             |     |     |       |               |     |     |
|-------------|-----|-----|-------|---------------|-----|-----|
| Application | Php | Php | 5.0   | rc3           | All | All |
| Application | Php | Php | 5.0.0 | All           | All | All |
| Application | Php | Php | 5.0.0 | beta1         | All | All |
| Application | Php | Php | 5.0.0 | beta2         | All | All |
| Application | Php | Php | 5.0.0 | beta3         | All | All |
| Application | Php | Php | 5.0.0 | beta4         | All | All |
| Application | Php | Php | 5.0.0 | rc1           | All | All |
| Application | Php | Php | 5.0.0 | rc2           | All | All |
| Application | Php | Php | 5.0.0 | rc3           | All | All |
| Application | Php | Php | 5.0.1 | All           | All | All |
| Application | Php | Php | 5.0.2 | All           | All | All |
| Application | Php | Php | 5.0.3 | All           | All | All |
| Application | Php | Php | 5.0.4 | All           | All | All |
| Application | Php | Php | 5.0.5 | All           | All | All |
| Application | Php | Php | 5.1.0 | All           | All | All |
| Application | Php | Php | 5.1.1 | All           | All | All |
| Application | Php | Php | 5.1.2 | All           | All | All |
| Application | Php | Php | 5.1.3 | All           | All | All |
| Application | Php | Php | 5.1.4 | All           | All | All |
| Application | Php | Php | 5.1.5 | All           | All | All |
| Application | Php | Php | 5.1.6 | All           | All | All |
| Application | Php | Php | 5.2.0 | All           | All | All |
| Application | Php | Php | 5.2.1 | All           | All | All |
| Application | Php | Php | 4.0   | All           | All | All |
| Application | Php | Php | 4.0   | beta1         | All | All |
| Application | Php | Php | 4.0   | beta2         | All | All |
| Application | Php | Php | 4.0   | beta3         | All | All |
| Application | Php | Php | 4.0   | beta4         | All | All |
| Application | Php | Php | 4.0   | beta_4_patch1 | All | All |
| Application | Php | Php | 4.0   | rc1           | All | All |
| Application | Php | Php | 4.0   | rc2           | All | All |
| Application | Php | Php | 4.0.0 | All           | All | All |
| Application | Php | Php | 4.0.1 | All           | All | All |
| Application | Php | Php | 4.0.1 | patch1        | All | All |
| Application | Php | Php | 4.0.1 | patch2        | All | All |
| Application | Php | Php | 4.0.0 | All           | All | All |

|             |     |     |        |        |     |     |
|-------------|-----|-----|--------|--------|-----|-----|
| Application | Php | Php | 4.0.2  | All    | All | All |
| Application | Php | Php | 4.0.3  | All    | All | All |
| Application | Php | Php | 4.0.3  | patch1 | All | All |
| Application | Php | Php | 4.0.4  | All    | All | All |
| Application | Php | Php | 4.0.4  | patch1 | All | All |
| Application | Php | Php | 4.0.5  | All    | All | All |
| Application | Php | Php | 4.0.6  | All    | All | All |
| Application | Php | Php | 4.0.7  | All    | All | All |
| Application | Php | Php | 4.0.7  | rc1    | All | All |
| Application | Php | Php | 4.0.7  | rc2    | All | All |
| Application | Php | Php | 4.0.7  | rc3    | All | All |
| Application | Php | Php | 4.1.0  | All    | All | All |
| Application | Php | Php | 4.1.1  | All    | All | All |
| Application | Php | Php | 4.1.2  | All    | All | All |
| Application | Php | Php | 4.2    | All    | dev | All |
| Application | Php | Php | 4.2.0  | All    | All | All |
| Application | Php | Php | 4.2.1  | All    | All | All |
| Application | Php | Php | 4.2.2  | All    | All | All |
| Application | Php | Php | 4.2.3  | All    | All | All |
| Application | Php | Php | 4.3.0  | All    | All | All |
| Application | Php | Php | 4.3.1  | All    | All | All |
| Application | Php | Php | 4.3.10 | All    | All | All |
| Application | Php | Php | 4.3.11 | All    | All | All |
| Application | Php | Php | 4.3.2  | All    | All | All |
| Application | Php | Php | 4.3.3  | All    | All | All |
| Application | Php | Php | 4.3.4  | All    | All | All |
| Application | Php | Php | 4.3.5  | All    | All | All |
| Application | Php | Php | 4.3.6  | All    | All | All |
| Application | Php | Php | 4.3.7  | All    | All | All |
| Application | Php | Php | 4.3.8  | All    | All | All |
| Application | Php | Php | 4.3.9  | 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 |



|                                                                                |           |                              |           |
|--------------------------------------------------------------------------------|-----------|------------------------------|-----------|
| cvs.php.net/viewvc.cgi/php-src/ext/gd/libgd/wbmp.c                             | MISC      | cvs.php.net                  |           |
| PHP GD Extension WBMP File Integer Overflow Vulnerabilities                    | BID       | www.securityfocus.com        |           |
| SecurityFocus                                                                  | BUGTRAQ   | www.securityfocus.com        |           |
| Advisories   Mandriva                                                          | MANDRIVA  | www.mandriva.com             |           |
| SUSE update for php - Advisories - Secunia                                     | SECUNIA   | secunia.com                  | Vendor A  |
| Support                                                                        | REDHAT    | www.redhat.com               | Vendor A  |
| APPLE-SA-2007-07-31 Security Update 2007-007                                   | APPLE     | lists.apple.com              |           |
| Gentoo Linux Documentation -- PHP: Multiple vulnerabilities                    | GENTOO    | security.gentoo.org          |           |
| Red Hat update for php - Advisories - Secunia                                  | SECUNIA   | secunia.com                  | Vendor A  |
| PHP: PHP 5.2.2 Release Announcement                                            | CONFIRM   | us2.php.net                  |           |
| rhn.redhat.com   Red Hat Support                                               | REDHAT    | rhn.redhat.com               | Vendor A  |
| The Slackware Linux Project: Slackware Security Advisories                     | SLACKWARE | www.slackware.org            |           |
| issues.rpath.com/browse/RPL-1268                                               | CONFIRM   | issues.rpath.com             |           |
| cvs.php.net/viewvc.cgi/php-src/ext/gd/libgd/wbmp.c                             | CONFIRM   | cvs.php.net                  |           |
| Slackware update for php - Advisories - Secunia                                | SECUNIA   | secunia.com                  | Vendor A  |
| PHP: PHP 4.4.7 Release Announcement                                            | CONFIRM   | us2.php.net                  |           |
| Red Hat update for php - Advisories - Secunia                                  | SECUNIA   | secunia.com                  | Vendor A  |
| Security Announcement                                                          | SUSE      | www.novell.com               |           |
| Webmail - OVH                                                                  | VUPEN     | www.vupen.com                | Vendor A  |
| IBM X-Force Exchange                                                           | XF        | exchange.xforce.ibmcloud.com |           |
| Support                                                                        | REDHAT    | www.redhat.com               | Vendor A  |
| Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia | SECUNIA   | secunia.com                  | Vendor A  |
| Advisories   Mandriva                                                          | MANDRIVA  | www.mandriva.com             |           |
| PHP "readwbmp()" Integer Overflow Vulnerability - Advisories - Secunia         | SECUNIA   | secunia.com                  | Vendor A  |
| Advisories   Mandriva                                                          | MANDRIVA  | www.mandriva.com             |           |
| Ivan Fratric's Security Blog: PHP <= 5.2.1 wbmp file handling integer overflow | MISC      | ifsec.blogspot.com           |           |
| Repository / Oval Repository                                                   | OVAL      | oval.cisecurity.org          |           |
| Apple Mac OS X 2007-007 Multiple Security Vulnerabilities                      | BID       | www.securityfocus.com        |           |
| Advisories   Mandriva                                                          | MANDRIVA  | www.mandriva.com             |           |
| Gentoo update for php - Advisories - Secunia                                   | SECUNIA   | secunia.com                  | Vendor A  |
| CVE Program record                                                             | CVE.ORG   | www.cve.org                  | canonical |
| NVD vulnerability detail                                                       | NVD       | nvd.nist.gov                 | canonical |

| Vendor Comments And Credit |            |             |                                                                                               |
|----------------------------|------------|-------------|-----------------------------------------------------------------------------------------------|
| Organization               | Published  | Contributor | Statement                                                                                     |
| Red Hat                    | 2008-02-14 | Mark J Cox  | This issue was fixed in php package updates for Red Hat Enterprise Linux and Red Hat Applicat |



There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)