



# CVE-2013-7226

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-7226                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | cve@mitre.org                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2014-02-18 11:55:00 UTC                                                                                                     |
| <b>Updated</b>         | 2023-11-07 02:17:00 UTC                                                                                                     |
| <b>Description</b>     | Integer overflow in the gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 allows remote attackers to cause a de |

## Risk And Classification

### Problem Types: CWE-189

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Php    | Php     | 5.5.0   | alpha1 | All     | All      |
| Application | Php    | Php     | 5.5.0   | alpha2 | All     | All      |
| Application | Php    | Php     | 5.5.0   | alpha3 | All     | All      |
| Application | Php    | Php     | 5.5.0   | alpha4 | All     | All      |
| Application | Php    | Php     | 5.5.0   | alpha5 | All     | All      |
| Application | Php    | Php     | 5.5.0   | alpha6 | All     | All      |
| Application | Php    | Php     | 5.5.0   | beta1  | All     | All      |
| Application | Php    | Php     | 5.5.0   | beta2  | All     | All      |
| Application | Php    | Php     | 5.5.0   | beta3  | All     | All      |
| Application | Php    | Php     | 5.5.0   | beta4  | All     | All      |
| Application | Php    | Php     | 5.5.0   | rc1    | All     | All      |
| Application | Php    | Php     | 5.5.0   | rc2    | All     | All      |
| Application | Php    | Php     | 5.5.1   | All    | All     | All      |
| Application | Php    | Php     | 5.5.2   | All    | All     | All      |
| Application | Php    | Php     | 5.5.3   | All    | All     | All      |
| Application | Php    | Php     | 5.5.4   | All    | All     | All      |
| Application | Php    | Php     | 5.5.5   | All    | All     | All      |

|             |                     |                     |       |        |     |     |
|-------------|---------------------|---------------------|-------|--------|-----|-----|
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.6 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.7 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.8 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | alpha1 | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | alpha2 | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | alpha3 | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | alpha4 | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | alpha5 | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | alpha6 | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | beta1  | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | beta2  | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | beta3  | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | beta4  | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | rc1    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.0 | rc2    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.1 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.2 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.3 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.4 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.5 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.6 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.7 | All    | All | All |
| Application | <a href="#">Php</a> | <a href="#">Php</a> | 5.5.8 | All    | All | All |

| References                                                                                                           |  |  |  |  |  |         |
|----------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|---------|
| Reference                                                                                                            |  |  |  |  |  | Source  |
| Security Advisory SA56829 - PHP &quot;imagecrop()&quot; Buffer Overflow Vulnerabilities - Secunia                    |  |  |  |  |  | SECUNIA |
| IBM X-Force Exchange                                                                                                 |  |  |  |  |  | XF      |
| 208.43.231.11 Git - php-src.git/commit                                                                               |  |  |  |  |  |         |
| PHP 'ext/gd/gd.c' Heap Based Buffer Overflow Vulnerability                                                           |  |  |  |  |  | BID     |
| Support / Security / Advisories / / MDVSA-2014:027   Mandriva                                                        |  |  |  |  |  | MANDRIV |
| Bug 1065108 – CVE-2013-7226 CVE-2013-7327 CVE-2013-7328 CVE-2014-2020 php: multiple vulnerabilities in gdImageCrop() |  |  |  |  |  | CONFIRM |
| PHP :: Sec Bug #66356 :: Heap Overflow Vulnerability in imagecrop()                                                  |  |  |  |  |  | CONFIRM |
| PHP Heap Overflow in imagecrop() Lets Remote Users Execute Arbitrary Code - SecurityTracker                          |  |  |  |  |  | SECTRAC |
| 208.43.231.11 Git - php-src.git/commit                                                                               |  |  |  |  |  | CONFIRM |
| CVE-2014-0085: PHP 5.5.8-RC1: Multiple Buffer Overflows in GD Library                                                |  |  |  |  |  | CONFIRM |

|                                                                                              |         |
|----------------------------------------------------------------------------------------------|---------|
| Fixed bug #66356 (Heap Overflow vulnerability in imagecrop()) · php/php-src@2938329 · GitHub | CONFIRM |
| PHP: PHP 5 ChangeLog                                                                         | CONFIRM |
| USN-2126-1: PHP vulnerabilities   Ubuntu                                                     | UBUNTU  |
| CVE Program record                                                                           | CVE.ORG |
| NVD vulnerability detail                                                                     | NVD     |

No vendor comments have been submitted for this CVE.

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](#)