



# CVE-2016-10168

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2016-10168  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | security@debian.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2017-03-15 15:59:00 UTC   |
| <b>Updated</b>         | 2018-05-04 01:29:00 UTC   |
| <b>Description</b>     | Integer overflow in gd_io.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified |

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Libgd  | Libgd   | All     | All    | All     | All      |

## References

| Reference  |
|--|
| Signed Integer Overflow gd_gd2.c · Issue #354 · libgd/libgd · GitHub   |
| Debian -- Security Information -- DSA-3777-1 libgd2  |
| oss-security - CVE Requests: libgd: potential unsigned onderflow, denial-of-service in gdImageCreateFromGd2Ctx and signed overflow in gd_  |
| LibGD 2.2.4 release  |
| libgd Multiple Security Vulnerabilities  |
| Red Hat Customer Portal  |
| Red Hat Customer Portal  |
| PHP Multiple Flaws Let Remote and Local Users Obtain Potentially Sensitive Information, Deny Service, and Execute Arbitrary Code - Securit |
| Fix #354: Signed Integer Overflow gd_io.c · libgd/libgd@69d2fd2 · GitHub   |
| oss-security - Re: CVE Requests: libgd: potential unsigned onderflow, denial-of-service in gdImageCreateFromGd2Ctx and signed overflow in  |
| CVE Program record   |
| NVD vulnerability detail   |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

378159 Virtuozzo Linux Security Update for php (VZLSA-2017:3221)

© [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](#).

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