



# CVE-2016-9398

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2016-9398   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2017-03-23 18:59:00 UTC   |
| <b>Updated</b>         | 2023-11-07 02:37:00 UTC   |
| <b>Description</b>     | The jpc_floorlog2 function in jpc_math.c in Jasper before 1.900.17 allows remote attackers to cause a denial of service (as |

## Risk And Classification

**Problem Types:** CWE-617

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                         | Product                                  | Version | Update | Edition | Language |
|------------------|--------------------------------|--|---------|--------|---------|----------|
| Operating System | <a href="#">Fedoraproject</a>  | <a href="#">Fedora</a>                   | 32      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a>  | <a href="#">Fedora</a>                   | 33      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a>  | <a href="#">Fedora</a>                   | 32      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a>  | <a href="#">Fedora</a>                   | 33      | All    | All     | All      |
| Application      | <a href="#">Jasper Project</a> | <a href="#">Jasper</a>                   | All     | All    | All     | All      |
| Application      | <a href="#">Jasper Project</a> | <a href="#">Jasper</a>                   | All     | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>       | <a href="#">Leap</a>                     | 15.1    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>       | <a href="#">Leap</a>                     | 15.2    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>       | <a href="#">Leap</a>                     | 42.1    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>       | <a href="#">Leap</a>                     | 42.2    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>       | <a href="#">Leap</a>                     | 15.1    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>       | <a href="#">Leap</a>                     | 15.2    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>       | <a href="#">Leap</a>                     | 42.1    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>       | <a href="#">Leap</a>                     | 42.2    | All    | All     | All      |
| Operating System | <a href="#">Suse</a>           | <a href="#">Linux Enterprise Desktop</a> | 12      | sp1    | All     | All      |
| Operating System | <a href="#">Suse</a>           | <a href="#">Linux Enterprise Desktop</a> | 12      | sp2    | All     | All      |
| Operating System | <a href="#">Suse</a>           | <a href="#">Linux Enterprise Desktop</a> | 12      | sp1    | All     | All      |

|                  |                      |   |    |     |     |     |
|------------------|----------------------|---|----|-----|-----|-----|
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Desktop</a>                  | 12 | sp2 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Server</a>                   | 12 | sp1 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Server</a>                   | 12 | sp2 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Server</a>                   | 12 | sp2 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Server</a>                   | 12 | sp1 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Server</a>                   | 12 | sp2 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Server</a>                   | 12 | sp2 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Software Development Kit</a> | 12 | sp1 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Software Development Kit</a> | 12 | sp2 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Software Development Kit</a> | 12 | sp1 | All | All |
| Operating System | <a href="#">Suse</a> | <a href="#">Linux Enterprise Software Development Kit</a> | 12 | sp2 | All | All |

## References

| Reference   | Source  | Link  | Tags |
|---|---------|---|------|
| [SECURITY] Fedora 32 Update: jasper-2.0.24-1.fc32 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | Ma   |
| [security-announce] SUSE-SU-2017:0084-1: important: Security update for                     | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           | Ma   |
| [security-announce] openSUSE-SU-2020:1517-1: moderate: Security update f                    | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           | Ma   |
| oss-security - Re: jasper: multiple assertion failures                                      | MLIST   | <a href="http://www.openwall.com">www.openwall.com</a>                | Ma   |
| 1396980 – (CVE-2016-9398) CVE-2016-9398 jasper: reachable assertion in jpc_floorlog2()      | CONFIRM | <a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>         | Iss  |
| [security-announce] openSUSE-SU-2020:1523-1: moderate: Security update f                    | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           | Ma   |
| JasPer CVE-2016-9398 Denial of Service Vulnerability  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>      | Thi  |
| [SECURITY] Fedora 32 Update: jasper-2.0.24-1.fc32 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |      |
| jasper: multiple Assertion failure   agostino's blog  | MISC    | <a href="https://blogs.gentoo.org">blogs.gentoo.org</a>               | Pa   |
| [SECURITY] Fedora 33 Update: jasper-2.0.24-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | Ma   |
| [security-announce] openSUSE-SU-2017:0101-1: important: Security update                     | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           | Ma   |
| [SECURITY] Fedora 33 Update: jasper-2.0.24-1.fc33 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |      |
| CVE Program record  | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                          | car  |
| NVD vulnerability detail  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                       | car  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[690456](#) Free Berkeley Software Distribution (FreeBSD) Security Update for jasper (6842ac7e-d250-11ea-b9b7-08002728f74c)

[750631](#) OpenSUSE Security Update for jasper (openSUSE-SU-2020:1523-1)

© [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](#)**