



CVE-2016-9591

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2016-9591 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-03-09 20:29:00 UTC |
| Updated | 2019-10-09 23:20:00 UTC |
| Description | JasPer before version 2.0.12 is vulnerable to a use-after-free in the way it decodes certain JPEG 2000 image files resulting |

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------------|--|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Jasper Project | Jasper | All | All | All | All |
| Application | Jasper Project | Jasper | All | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |

| | | | | | | |
|------------------|------------------------|--|-----|-----|-----|-----|
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|---|-------------------|
| JasPer: Multiple vulnerabilities (GLSA 201707-07) — Gentoo Security | GENTOO | security.gentoo.org | Third Party Advis |
| Red Hat Customer Portal | REDHAT | access.redhat.com | Third Party Advis |
| Debian -- Security Information -- DSA-3827-1 jasper | DEBIAN | www.debian.org | Third Party Advis |
| Bug 1406405 – CVE-2016-9591 jasper: use-after-free / double-free in JPC encoder | CONFIRM | bugzilla.redhat.com | Exploit, Issue Tr |
| JasPer CVE-2016-9591 Denial of Service Vulnerability | BID | www.securityfocus.com | Third Party Advis |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analy |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378165](#) Virtuozzo Linux Security Update for jasper-utils (VZLSA-2017:1208)

[710375](#) Gentoo Linux JasPer Multiple Vulnerabilities (GLSA 201707-07)

© [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