



# CVE-2016-9573

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

## Summary

<b>CVE</b>	CVE-2016-9573
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-08-01 06:29:00 UTC
<b>Updated</b>	2023-02-12 23:27:00 UTC
<b>Description</b>	An out-of-bounds read vulnerability was found in OpenJPEG 2.1.2, in the j2k_to_image tool. Converting a specially crafted

## Risk And Classification

**Problem Types:** CWE-125

## 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
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	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 Server Eus	7.5	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	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Application	<a href="#">Uclouvain</a>	<a href="#">Openjpeg</a>	2.1.2	All	All	All
Application	<a href="#">Uclouvain</a>	<a href="#">Openjpeg</a>	2.1.2	All	All	All

## References

Reference	Source	Li
OpenJPEG: Multiple vulnerabilities (GLSA 201710-26) — Gentoo security	GENTOO	se
CVE-2016-9573 - Red Hat Customer Portal	MISC	ac
1402711 – (CVE-2016-9573) CVE-2016-9573 openjpeg: heap out-of-bounds read due to insufficient check in imagetopnm()	MISC	bu
Red Hat Customer Portal	MISC	ac
1402711 – (CVE-2016-9573) CVE-2016-9573 openjpeg: heap out-of-bounds read due to insufficient check in imagetopnm()	CONFIRM	bu
OpenJPEG CVE-2016-9573 Out of Bounds Read Denial of Service Vulnerability	BID	ww
Red Hat Customer Portal	REDHAT	rhi
Debian -- Security Information -- DSA-3768-1 openjpeg2	DEBIAN	ww
Changes for issues #863 and #862 · szukw000/openjpeg@7b28bd2 · GitHub	CONFIRM	git
Openjpeg-2.1.2 Heap Buffer Overflow Vulnerability due to Insufficient check · Issue #862 · uclouvain/openjpeg · GitHub	CONFIRM	git
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[378259](#) Virtuozzo Linux Security Update for openjpeg (VZLSA-2017:0838)

[710394](#) Gentoo Linux OpenJPEG Multiple Vulnerabilities (GLSA 201710-26)

© [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](#)