



# CVE-2018-16376

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

## Summary

<b>CVE</b>	CVE-2018-16376
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-09-03 00:29:00 UTC
<b>Updated</b>	2018-10-31 14:26:00 UTC
<b>Description</b>	An issue was discovered in OpenJPEG 2.3.0. A heap-based buffer overflow was discovered in the function t2_encode_packet

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Uclouvain	Openjpeg	2.3.0	All	All	All
Application	Uclouvain	Openjpeg	2.3.0	All	All	All

## References

Reference	Source
OpenJPEG CVE-2018-16376 Remote Heap Based Buffer Overflow Vulnerability	BID
Potential heap-based buffer overflow in function t2_encode_packet in src/lib/openmj2/t2.c · Issue #1127 · uclouvain/openjpeg · GitHub	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[751971](#) SUSE Enterprise Linux Security Update for openjpeg2 (SUSE-SU-2022:1129-1)

[752044](#) SUSE Enterprise Linux Security Update for openjpeg2 (SUSE-SU-2022:1252-1)

[752060](#) SUSE Enterprise Linux Security Update for openjpeg (SUSE-SU-2022:1296-1)

---

© [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](#)**