



# CVE-2020-8112

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

## Summary

<b>CVE</b>	CVE-2020-8112
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-28 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:26:00 UTC
<b>Description</b>	opj_t1_clbl_decode_processor in openjp2/t1.c in OpenJPEG 2.3.1 through 2020-01-28 has a heap-based buffer overflow in

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Uclouvain</a>	<a href="#">Openjpeg</a>	2.3.1	All	All	All
Application	<a href="#">Uclouvain</a>	<a href="#">Openjpeg</a>	2.3.1	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
[SECURITY] Fedora 31 Update: mingw-openjpeg2-2.3.1-7.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
Oracle Critical Patch Update Advisory - July 2020	MISC	<a href="#">www.oracle.com</a>
[SECURITY] Fedora 30 Update: mingw-openjpeg2-2.3.1-7.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: mingw-openjpeg2-2.3.1-7.fc30 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
Another heap buffer overflow in libopenjp2 · Issue #1231 · uclouvain/openjpeg · GitHub	MISC	<a href="#">github.com</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
[SECURITY] [DLA 2089-1] openjpeg2 security update	MLIST	<a href="#">lists.debian.org</a>
Debian -- Security Information -- DSA-4882-1 openjpeg2	DEBIAN	<a href="#">www.debian.org</a>

[SECURITY] Fedora 31 Update: mingw-openjpeg2-2.3.1-7.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
[SECURITY] [DLA 2277-1] openjpeg2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [178518](#) Debian Security Update for openjpeg2 (DSA 4882-1)
- [199240](#) Ubuntu Security Notification for OpenJPEG Vulnerabilities (USN-5952-1)
- [20277](#) Oracle Database 18c Critical OJVM Patch Update - July 2020
- [377073](#) Alibaba Cloud Linux Security Update for openjpeg2 (ALINUX2-SA-2020:0022)
- [377111](#) Alibaba Cloud Linux Security Update for openjpeg2 (ALINUX3-SA-2022:0096)
- [500471](#) Alpine Linux Security Update for openjpeg
- [504228](#) Alpine Linux Security Update for openjpeg
- [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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)