



CVE-2018-20846

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

Summary

CVE	CVE-2018-20846
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-26 18:15:00 UTC
Updated	2023-02-27 16:48:00 UTC
Description	Out-of-bounds accesses in the functions pi_next_lrcp, pi_next_rlcp, pi_next_rpcl, pi_next_pcl, pi_next_rpcl, and pi_next_cp

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Fix multiple potential vulnerabilities and bugs by Young-X · Pull Request #1168 · uclouvain/openjpeg · GitHub	MISC	github.com
OpenJPEG Multiple Security Vulnerabilities	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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)

[752740](#) SUSE Enterprise Linux Security Update for openjpeg2 (SUSE-SU-2022:3802-1)

[752823](#) SUSE Enterprise Linux Security Update for openjpeg (SUSE-SU-2022:4082-1)

© [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](#)