



CVE-2023-2617

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-2617 |
| State | PUBLIC |
| Assigner | cna@vuldb.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-05-10 06:15:00 UTC |
| Updated | 2023-11-07 04:12:00 UTC |
| Description | A vulnerability classified as problematic was found in OpenCV wechat_qrcode Module up to 4.7.0. Affected by this vulnerat |

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Opencv | Opencv | All | All | All | All |

References

Reference

Login required

qrcode_crash_wechat.py · GitHub

CVE-2023-2617: OpenCV wechat_qrcode Module decoded_bit_stream_parser.cpp decodeByteSegment null pointer dereference (ID 3480)

fix(wechat_qrcode): Init nBytes after the count value is determined by Konano · Pull Request #3480 · opencv/opencv_contrib · GitHub

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184305 Debian Security Update for opencv (CVE-2023-2617)

© [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](#)