CVE-2017-18009

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-18009
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-01 08:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	In OpenCV 3.3.1, a heap-based buffer over-read exists in the function cv::HdrDecoder::checkSignature in modules/imgcode

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opencv	Opencv	3.3.1	All	All	All
Application	Opencv	Opencv	3.3.1	All	All	All

References

Reference	Source	Link	Tags
Buffer overflow in cv::HdrDecoder::checkSignature · Issue #10479 · opencv/opencv · GitHub	MISC	github.com	Issue T
OpenCV Denial of Service and Heap Buffer Overflow Vulnerabilities	BID	www.securityfocus.com	Third P
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980432 Python (pip) Security Update for opencv-contrib-python (GHSA-83rh-hx5x-q9p5)

© 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 registred 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