



CVE-2017-13735

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

Summary

CVE	CVE-2017-13735
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-29 06:29:00 UTC
Updated	2017-08-30 15:17:00 UTC
Description	There is a floating point exception in the kodak_radc_load_raw function in ddraw_common.cpp in LibRaw 0.18.2. It will lead

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libraw	Libraw	0.18.2	All	All	All
Application	Libraw	Libraw	0.18.2	All	All	All

References

Reference	Source	L
1483988 – There is a floating point exception in ddraw_common.cpp of libRAW. It will lead to remote denial of service attack.	MISC	b
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[179045](#) Debian Security Update for libraw (DLA 2903-1)

[501048](#) Alpine Linux Security Update for libraw

[505014](#) Alpine Linux Security Update for libraw

[752153](#) SUSE Enterprise Linux Security Update for ddraw (SUSE-SU-2022:1749-1)

© [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](#)