



CVE-2021-36083

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

Summary

CVE	CVE-2021-36083
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-01 03:15:00 UTC
Updated	2021-07-08 17:36:00 UTC
Description	KDE KImageFormats 5.70.0 through 5.81.0 has a stack-based buffer overflow in XCFImageFormat::loadTileRLE.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kde	Kimageformats	All	All	All	All

References

Reference	Source	Link
33742 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chro
xcf: Fix Stack-buffer-overflow WRITE on broken files (297ed9a2) · Commits · Frameworks / KImageFormats · GitLab	MISC	invent.kd
oss-fuzz-vulns/OSV-2021-695.yaml at main · google/oss-fuzz-vulns · GitHub	MISC	github.co
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[179399](#) Debian Security Update for kimageformats (CVE-2021-36083)

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](#)