



CVE-2023-27103

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-27103
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-15 15:15:00 UTC
Updated	2023-11-30 19:15:00 UTC
Description	Libde265 v1.0.11 was discovered to contain a heap buffer overflow via the function derive_collocated_motion_vectors at m

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Struktur	Libde265	1.0.11	All	All	All

References

Reference

- [debian-lts-announce] 20231130 [SECURITY] [DLA 3676-1] libde265 security update
- A heap-buffer-overflow has occurred when running program dec265 in function derive_collocated_motion_vectors at motion.cc · Issue #394 · s
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 200168 Ubuntu Security Notification for libde265 Vulnerabilities (USN-6677-1)
- 502698 Alpine Linux Security Update for libde265
- 504055 Alpine Linux Security Update for libde265
- 6000362 Debian Security Update for libde265 (DLA 3676-1)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)