



CVE-2023-25221

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

Summary

CVE	CVE-2023-25221
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-01 15:15:00 UTC
Updated	2023-03-10 18:23:00 UTC
Description	Libde265 v1.0.10 was discovered to contain a heap-buffer-overflow vulnerability in the derive_spatial_luma_vector_prediction function.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Struktur	Libde265	1.0.10	All	All	All

References

Reference	Source
heap-buffer-overflow in function derive_spatial_luma_vector_prediction at motion.cc:1894 · Issue #388 · strukturag/libde265 · GitHub	MISC
[SECURITY] [DLA 3352-1] libde265 security update	MLIST
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181622](#) Debian Security Update for libde265 (DLA 3352-1)

[184587](#) Debian Security Update for libde265 (CVE-2023-25221)

[200138](#) Ubuntu Security Notification for libde265 Vulnerabilities (USN-6659-1)

© [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](#)