



# CVE-2023-24755

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

## Summary

<b>CVE</b>	CVE-2023-24755
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-01 15:15:00 UTC
<b>Updated</b>	2023-03-10 18:18:00 UTC
<b>Description</b>	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the put_weighted_pred_8_fallback function at fa

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Application	<a href="#">Struktur</a>	<a href="#">Libde265</a>	1.0.10	All	All	All

## References

Reference	Source
NULL Pointer Dereference in function put_weighted_pred_8_fallback at fallback-motion.cc:69 · Issue #384 · strukturag/libde265 · GitHub	MI
[SECURITY] [DLA 3352-1] libde265 security update	MI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- [181622](#) Debian Security Update for libde265 (DLA 3352-1)
- [182819](#) Debian Security Update for libde265 (CVE-2023-24755)
- [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](#)