



# CVE-2022-47665

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-47665
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-03 15:15:00 UTC
<b>Updated</b>	2023-03-10 19:22:00 UTC
<b>Description</b>	Libde265 1.0.9 has a heap buffer overflow vulnerability in de265_image::set_SliceAddrRS(int, int, int)

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Struktur	Libde265	1.0.9	All	All	All

## References

### Reference

heap-buffer-overflow (libde265/build/libde265/libde265.so+0x1ec50d) in de265\_image::set\_SliceAddrRS(int, int, int) · Issue #369 · strukturag/

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[182894](#) Debian Security Update for libde265 (CVE-2022-47665)

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)