



# CVE-2022-43240

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

## Summary

<b>CVE</b>	CVE-2022-43240
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-02 14:15:00 UTC
<b>Updated</b>	2023-02-27 15:24:00 UTC
<b>Description</b>	Libde265 v1.0.8 was discovered to contain a heap-buffer-overflow vulnerability via ff_hevc_put_hevc_qpel_h_2_v_1_sse in

## Risk And Classification

**Problem Types:** CWE-787

## 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
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Application	<a href="#">Struktur</a>	<a href="#">Libde265</a>	1.0.8	All	All	All

## References

Reference	Source	Link
[SECURITY] [DLA 3280-1] libde265 security update	MLIST	<a href="#">lists.d</a>
Heap-buffer-overflow in sse-motion.cc: ff_hevc_put_hevc_qpel_h_2_v_1_sse · Issue #335 · strukturag/libde265 · GitHub	MISC	<a href="#">github</a>
Debian -- Security Information -- DSA-5346-1 libde265	DEBIAN	<a href="#">www.</a>
CVE Program record	CVE.ORG	<a href="#">www.</a>
NVD vulnerability detail	NVD	<a href="#">nvd.n</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[181500](#) Debian Security Update for libde265 (DLA 3280-1)

[181556](#) Debian Security Update for libde265 (DSA 5346-1)

183269 Debian Security Update for libde265 (CVE-2022-43240)
200101 Ubuntu Security Notification for libde265 Vulnerabilities (USN-6627-1)
502651 Alpine Linux Security Update for libde265
504054 Alpine Linux Security Update for libde265
691071 Free Berkeley Software Distribution (FreeBSD) Security Update for libde256 (421c0af9-b206-11ed-9fe5-f4a47516fb57)

© [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](#)