



CVE-2020-21605

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

Summary

CVE	CVE-2020-21605
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-16 22:15:00 UTC
Updated	2023-02-11 13:15:00 UTC
Description	libde265 v1.0.4 contains a segmentation fault in the apply_sao_internal function, which can be exploited via a crafted a file.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libde265	Libde265	1.0.4	All	All	All
Application	Struktur	Libde265	1.0.4	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-5346-1 libde265	DEBIAN	www.debian.org	
segment fault in apply_sao_internal when decoding file · Issue #234 · strukturag/libde265 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

[200084](#) Ubuntu Security Notification for libde265 Vulnerabilities (USN-6617-1)

[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](#)