



CVE-2022-2832

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

Summary

CVE	CVE-2022-2832
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-16 21:15:00 UTC
Updated	2023-02-12 22:15:00 UTC
Description	A flaw was found in Blender 3.3.0. A null pointer dereference exists in source/blender/gpu/opengl/gl_backend.cc that may k

Risk And Classification

Problem Types: CWE-395

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Blender	Blender	3.3.0	alpha	All	All

References

Reference	Source	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
⚓ T99706 Null pointer Reference in blender_headless	MISC	developer.blender
2118556 – (CVE-2022-2832) CVE-2022-2832 blender: Null pointer reference in blender thumbnail extractor	MISC	bugzilla.redhat.cor
rB00dc7477022a	MISC	developer.blender
⚙ D15463 Fix T99706: Crash rendering with headless builds	MISC	developer.blender
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

502820 Alpine Linux Security Update for blender

© [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](#)