



CVE-2023-33865

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

Summary

CVE	CVE-2023-33865
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-07 20:15:00 UTC
Updated	2023-08-02 16:43:00 UTC
Description	RenderDoc before 1.27 allows local privilege escalation via a symlink attack. It relies on the /tmp/RenderDoc directory rega

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Renderdoc	Renderdoc	All	All	All	All
Application	Renderdoc	Renderdoc	All	All	All	All

References

Reference	Source	Link
RenderDoc 1.26 Local Privilege Escalation / Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com
www.qualys.com/2023/06/06/renderdoc/renderdoc.txt	MISC	www.qualys.com
RenderDoc	MISC	renderdoc.org
Full Disclosure: LPE and RCE in RenderDoc: CVE-2023-33865, CVE-2023-33864, CVE-2023-33863	FULLDISC	seclists.org
[SECURITY] [DLA 3501-1] renderdoc security update	MLIST	lists.debian.org
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

[6000152](#) Debian Security Update for renderdoc (DLA 3501-1)

© [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](#)