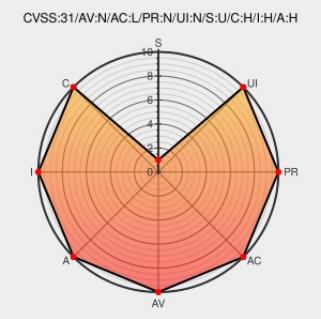
CVE-2023-33864

Published on: Not Yet Published

Last Modified on: 08/02/2023 04:44:00 PM UTC

CVE-2023-33864

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Renderdoc from Renderdoc contain the following vulnerability:

StreamReader::ReadFromExternal in RenderDoc before 1.27 allows an Integer Overflow with a resultant Buffer Overflow. It uses uint32_t(m_BufferSize-m_InputSize) even though m_InputSize can exceed m_BufferSize.

CVE-2023-33864 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
RenderDoc 1.26 Local Privilege Escalation / Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/172804/RenderDoc-1.26-Local-Privilege-Escalation-Remote-Code-Execution.html
	www.qualys.com text/plain	MISC www.qualys.com/2023/06/06/renderdoc/renderdoc.txt
RenderDoc	renderdoc.org text/html	MISC renderdoc.org/
Full Disclosure: LPE and RCE in RenderDoc: CVE-2023-33865, CVE-2023-33864, CVE-2023-33863	seclists.org text/html	FULLDISC 20230607 LPE and RCE in RenderDoc: CVE-2023-33865, CVE-2023-33864, CVE-2023-33863
[SECURITY] [DLA 3501-1] renderdoc security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20230725 [SECURITY] [DLA 3501-1] renderdoc security update

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

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

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:renderdoc:renderdoc:*:*:*:*:*:*:*:*:

cpe:2.3:a:renderdoc:renderdoc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→