



# CVE-2022-0135

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

## Summary

<b>CVE</b>	CVE-2022-0135
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-25 18:15:00 UTC
<b>Updated</b>	2023-02-03 19:05:00 UTC
<b>Description</b>	An out-of-bounds write issue was found in the VirGL virtual OpenGL renderer (virglrenderer). This flaw allows a malicious g

## 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="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Application	<a href="#">Virglrenderer Project</a>	<a href="#">Virglrenderer</a>	All	All	All	All

## References

Reference	Source	Link
2037790 – (CVE-2022-0135) CVE-2022-0135 virglrenderer: out-of-bounds write in read_transfer_data()	MISC	<a href="#">bugzilla.redhat.com</a>
[SECURITY] [DLA 3232-1] virglrenderer security update	MLIST	<a href="#">lists.debian.org</a>
virglrenderer: Multiple vulnerabilities (GLSA 202210-05) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[181309](#) Debian Security Update for virglrenderer (DLA 3232-1)

[181429](#) Debian Security Update for virglrenderer (CVE-2022-0135)

<a href="#">198682</a> Ubuntu Security Notification for virglrenderer Vulnerabilities (USN-5309-1)
<a href="#">502962</a> Alpine Linux Security Update for virglrenderer
<a href="#">505829</a> Alpine Linux Security Update for virglrenderer
<a href="#">710637</a> Gentoo Linux virglrenderer Multiple Vulnerabilities (GLSA 202210-05)
<a href="#">751715</a> SUSE Enterprise Linux Security Update for virglrenderer (SUSE-SU-2022:0478-1)
<a href="#">751718</a> SUSE Enterprise Linux Security Update for virglrenderer (SUSE-SU-2022:0479-1)
<a href="#">751753</a> OpenSUSE Security Update for virglrenderer (openSUSE-SU-2022:0479-1)
<a href="#">753478</a> SUSE Enterprise Linux Security Update for virglrenderer (SUSE-SU-2022:2395-1)
<a href="#">903880</a> Common Base Linux Mariner (CBL-Mariner) Security Update for virglrenderer (10724) (DEPRECATED)
<a href="#">903920</a> Common Base Linux Mariner (CBL-Mariner) Security Update for virglrenderer (10724-1)

© [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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)