



CVE-2022-0175

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

Summary

CVE	CVE-2022-0175
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-26 18:15:00 UTC
Updated	2022-11-08 03:02:00 UTC
Description	A flaw was found in the VirGL virtual OpenGL renderer (virglrenderer). The virgl did not properly initialize memory when alloc

Risk And Classification

Problem Types: CWE-909

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Virglrenderer Project	Virglrenderer	All	All	All	All
Application	Virglrenderer Project	Virglrenderer	0.9.0	All	All	All
Application	Virglrenderer Project	Virglrenderer	0.9.1	All	All	All

References

Reference

- [Red Hat Customer Portal - Access to 24x7 support and knowledge](#)
- [2039003 – \(CVE-2022-0175\) CVE-2022-0175 virglrenderer: memory initialization issue in vrend_resource_alloc_buffer\(\) can lead to info leak](#)
- [Fix a number of security issues \(I654\) · Merge requests · virgl / virglrenderer · GitLab](#)
- [vrend: clear memory when allocating a host-backed memory resource \(b05bb61f\) · Commits · virgl / virglrenderer · GitLab](#)
- [CVE-2022-0175](#)
- [virglrenderer: Multiple vulnerabilities \(GLSA 202210-05\) — Gentoo security](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

198682	Ubuntu Security Notification for virglrenderer Vulnerabilities (USN-5309-1)
502962	Alpine Linux Security Update for virglrenderer
505829	Alpine Linux Security Update for virglrenderer
710637	Gentoo Linux virglrenderer Multiple Vulnerabilities (GLSA 202210-05)
751609	SUSE Enterprise Linux Security Update for virglrenderer (SUSE-SU-2022:0110-1)
751615	OpenSUSE Security Update for virglrenderer (openSUSE-SU-2022:0111-1)
753088	SUSE Enterprise Linux Security Update for virglrenderer (SUSE-SU-2022:0111-1)
903860	Common Base Linux Mariner (CBL-Mariner) Security Update for virglrenderer (10772)
904142	Common Base Linux Mariner (CBL-Mariner) Security Update for virglrenderer (10772-1)

© [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](#)