



CVE-2016-10214

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

Summary

CVE	CVE-2016-10214
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-20 16:59:00 UTC
Updated	2017-07-11 01:33:00 UTC
Description	Memory leak in the virgl_resource_attach_backing function in virglrenderer before 0.6.0 allows local guest OS users to cause

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Virglrenderer Project	Virglrenderer	All	All	All	All

References

Reference	Source	Link
QEMU CVE-2016-10214 Denial of Service Vulnerability	BID	www.securityfocus.com/bid/78844
virglrenderer: Multiple vulnerabilities (GLSA 201707-06) — Gentoo security	GENTOO	security.gentoo.org/glsa/201707-06
[virglrenderer-devel] [ANNOUNCE] virglrenderer 0.6.0	MLIST	lists.freedesktop.org/archives/virglrenderer-devel/20170701000000.html
oss-security - Re: CVE request virglrenderer: host memory leak issue in virgl_resource_attach_backing	MLIST	www.openwall.com/lists/oss-security/2017/03/20/1
virglrenderer - VirGL virtual OpenGL renderer (mirrored from https://gitlab.freedesktop.org/virgl/virglrenderer)	CONFIRM	cgit.freedesktop.org/virgl/virglrenderer
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

[710490](#) Gentoo Linux virglrenderer Multiple Vulnerabilities (GLSA 201707-06)

© [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](#)