



CVE-2021-3611

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

Summary

CVE	CVE-2021-3611
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-11 16:15:00 UTC
Updated	2023-02-12 23:41:00 UTC
Description	A stack overflow vulnerability was found in the Intel HD Audio device (intel-hda) of QEMU. A malicious guest could use this

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
1973784 – (CVE-2021-3611) CVE-2021-3611 QEMU: intel-hda: segmentation fault due to stack overflow	MISC	bugzilla.redhat.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
CVE-2021-3611 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	security.gentoo.org
Stack-overflow in ldl_le_dma through intel-hda (CVE-2021-3611) (#542) · Issues · QEMU / QEMU · GitLab	MISC	gitlab.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
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

160273 Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-2022-7967)
182451 Debian Security Update for qemu (CVE-2021-3611)
240913 Red Hat Update for qemu-kvm security (RHSA-2022:7967)
710604 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
750874 OpenSUSE Security Update for qemu (openSUSE-SU-2021:2442-1)
750879 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:2448-1)
750889 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:2461-1)
750901 OpenSUSE Security Update for qemu (openSUSE-SU-2021:2474-1)
750903 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:2546-1)
750904 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:2563-1)
750910 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:2591-1)
750912 OpenSUSE Security Update for qemu (openSUSE-SU-2021:2591-1)
751053 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1202-1)
901584 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9745)
901868 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9744)
940832 AlmaLinux Security Update for qemu-kvm (ALSA-2022:7967)
960500 Rocky Linux Security Update for qemu-kvm (RLSA-2022:7967)

© [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](#)