



CVE-2020-13800

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-13800
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-04 16:15:00 UTC
Updated	2022-04-28 19:30:00 UTC
Description	ati-vga in hw/display/ati.c in QEMU 4.2.0 allows guest OS users to trigger infinite recursion via a crafted mm_index value d

Risk And Classification

Problem Types: CWE-674

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Qemu	Qemu	4.2.0	All	All	All
Application	Qemu	Qemu	4.2.0	All	All	All

References

Reference	Source	Link
June 2020 QEMU Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.c
QEMU: Multiple vulnerabilities (GLSA 202011-09) — Gentoo security	GENTOO	security.gentoo.o
USN-4467-1: QEMU vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
oss-security - CVE-2020-13800 QEMU: ati-vga: infinite recursion in ati_mm_read/write calls may lead to DoS	CONFIRM	www.openwall.co
[PATCH v2] ati-vga: check mm_index before recursive call	MISC	lists.gnu.org
Ingress Default Backend - 404 Not Found	MISC	cve.openeuler.org
[security-announce] openSUSE-SU-2020:1108-1: important: Security update	SUSE	lists.opensuse.org
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[502351](#) Alpine Linux Security Update for qemu

[900187](#) CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

[903384](#) Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1952)

© [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](#)