CVE-2020-13791

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-13791
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-04 16:15:00 UTC
Updated	2020-12-14 20:40:00 UTC
Description	hw/pci/pci.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access by providing an address near the end

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link
[PATCH] pci: check address before reading configuration bytes	MISC	lists.gnu.org
June 2020 QEMU Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.
QEMU: Multiple vulnerabilities (GLSA 202011-09) — Gentoo security	GENTOO	security.gentoo.
oss-security - CVE-2020-13791 QEMU: ati-vga: OOB access while reading PCI configuration may lead to DoS	CONFIRM	www.openwall.c
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

502351 Alpine Linux Security Update for qemu

900187 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

903308 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1965)