



CVE-2022-35414

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

Summary

CVE	CVE-2022-35414
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-11 02:15:00 UTC
Updated	2023-11-07 03:49:00 UTC
Description	** DISPUTED ** softmmu/physmem.c in QEMU through 7.0.0 can perform an uninitialized read on the translate_fail path, le

Risk And Classification

Problem Types: CWE-908

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference

- CVE-2022-35414 - QEMU 4.1.50 through QEMU 7.0.0 - address_space_translate_for_iotlb allows a guest user to crash a host resulting in a d
qemu/cpu-all.h at v7.0.0 · qemu/qemu · GitHub
- target/loongarch: Clean up tlb when cpu reset · qemu/qemu@3517fb7 · GitHub
- [SECURITY] [DLA 3099-1] qemu security update
- cpultb: uninitialized local variable in tlb_set_page_with_attrs cause SIGSEGV when a CPU access an unmapped IOMMU page (#1065) · Issu
- softmmu: Always initialize xlat in address_space_translate_for_iotlb · qemu/qemu@418ade7 · GitHub
- target/loongarch: Clean up tlb when cpu reset · qemu/qemu@3517fb7 · GitHub
- Security — QEMU documentation
- qemu/physmem.c at f200ff158d5abcb974a6b597a962b6b2f2bea2b06 · qemu/qemu · GitHub
- Re: [PATCH v2] softmmu: Always initialize xlat in address_space_translate_for_iotlb
- Re: [PATCH v2] softmmu: Always initialize xlat in address_space_translate_for_iotlb
- CVE Program record

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180995	Debian Security Update for qemu (DLA 3099-1)
184828	Debian Security Update for qemu (CVE-2022-35414)
752675	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3594-1)
752685	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3660-1)
752725	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3768-1)
752746	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3795-1)
753802	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0761-1)
902514	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (10123)
902556	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (10110)
903959	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (10110-1)
904012	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (10123-1)

© [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](#)