



# CVE-2017-11334

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

## Summary

<b>CVE</b>	CVE-2017-11334
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-08-02 19:29:00 UTC
<b>Updated</b>	2020-11-10 18:32:00 UTC
<b>Description</b>	The address_space_write_continue function in exec.c in QEMU (aka Quick Emulator) allows local guest OS privileged user

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party /
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party /
USN-3575-1: QEMU vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party /
Bug 1471638 – CVE-2017-11334 Qemu: exec: oob access during dma operation	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Trackin
oss-security - CVE-2017-11334 Qemu: exec: oob access during dma operation	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	Mailing List,
[Qemu-devel] [PULL 21/41] exec: use qemu_ram_ptr_length to access guest	MLIST	<a href="https://lists.gnu.org">lists.gnu.org</a>	Mailing List,
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party /
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party /
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party /
QEMU CVE-2017-11334 Out of Bounds Read and Write Denial of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party /
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party /

Debian -- Security Information -- DSA-3925-1 qemu	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Party A
Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.com</a>	Third Party A
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

900063 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)