



CVE-2017-11434

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

Summary

CVE	CVE-2017-11434
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-25 18:29:00 UTC
Updated	2020-11-10 17:48:00 UTC
Description	The dhcp_decode function in slirp/bootp.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	2.10.0	rc0	All	All
Application	Qemu	Qemu	2.10.0	rc1	All	All
Application	Qemu	Qemu	2.10.0	rc2	All	All
Application	Qemu	Qemu	2.10.0	rc3	All	All
Application	Qemu	Qemu	2.10.0	rc0	All	All
Application	Qemu	Qemu	2.10.0	rc1	All	All
Application	Qemu	Qemu	2.10.0	rc2	All	All
Application	Qemu	Qemu	2.10.0	rc3	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link	Tags
[Qemu-devel] [PATCH] slirp: check len against dhcp options array end	MLIST	lists.gnu.org	Issue

[SECURITY] [DLA 1497-1] qemu security update	MLIST	lists.debian.org	Third F
QEMU CVE-2017-11434 Out-of-Bounds Read Vulnerability	BID	www.securityfocus.com	Third F
Bug 1472611 – CVE-2017-11434 Qemu: slirp: out-of-bounds read while parsing dhcp options	CONFIRM	bugzilla.redhat.com	Issue
oss-security - CVE-2017-11434 Qemu: slirp: out-of-bounds read while parsing dhcp options	MLIST	www.openwall.com	Mailing
Debian -- Security Information -- DSA-3925-1 qemu	DEBIAN	www.debian.org	Third F
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

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](#) 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