

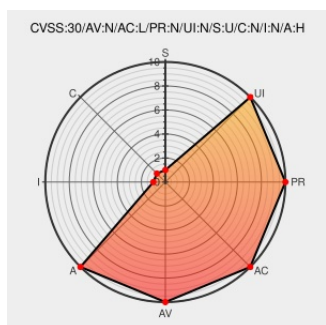


CVE-2018-17962

Published on: 10/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:20 PM UTC

CVE-2018-17962

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Qemu has a Buffer Overflow in pcnet_receive in hw/net/pcnet.c because an incorrect integer data type is used.

CVE-2018-17962 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 1599-1] qemu security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20181130 [SECURITY] [DLA 1599-1] qemu security update
CVE-2018-17962 - Red Hat Customer Portal	Third Party Advisory	MISC access.redhat.com/security/cve/cve-2018-17962

	access.redhat.com text/html	
oss-security - Qemu: integer overflow issues	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20181008 Qemu: integer overflow issues
USN-3826-1: QEMU vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3826-1
CVE-2018-17962 SUSE	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 MISC www.suse.com/security/cve/CVE-2018-17962/
[Qemu-devel] [PULL 23/25] pcnet: fix possible buffer overflow	Exploit Mailing List Third Party Advisory lists.gnu.org text/x-diff	 MLIST [qemu-devel] 20180926 [PULL 23/25] pcnet: fix possible buffer overflow
Debian -- Security Information -- DSA-4338-1 qemu	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4338
linux.oracle.com CVE-2018-17962	Third Party Advisory linux.oracle.com text/html	 MISC linux.oracle.com/cve/CVE-2018-17962.html
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:2892
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
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	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
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	18.10	All	All	All
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
Operating System	Oracle	Linux	7	0	All	All
Operating System	Oracle	Linux	7	0	All	All
Application	Qemu	Qemu	2.1.0	All	All	All
Application	Qemu	Qemu	2.12.0	All	All	All
Application	Qemu	Qemu	2.8.0	All	All	All
Application	Qemu	Qemu	2.1.0	All	All	All
Application	Qemu	Qemu	2.12.0	All	All	All
Application	Qemu	Qemu	2.8.0	All	All	All
Operating System	Redhat	Linux	6.0	All	All	All
Operating System	Redhat	Linux	6.0	All	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	All	All	All
Operating System	Suse	Linux Enterprise Server	15	All	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	All	All	All
Operating System	Suse	Linux Enterprise Server	15	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:its:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:its:*:*:						

cpe:2.3:o:canonical:ubuntu_linux:16.04.*.*.*:lts.*.*.*
cpe:2.3:o:canonical:ubuntu_linux:18.04.*.*.*:lts.*.*.*
cpe:2.3:o:canonical:ubuntu_linux:18.10.*.*.*.*.*.*
cpe:2.3:o:canonical:ubuntu_linux:14.04.*.*.*:lts.*.*.*
cpe:2.3:o:canonical:ubuntu_linux:16.04.*.*.*:lts.*.*.*
cpe:2.3:o:canonical:ubuntu_linux:18.04.*.*.*:lts.*.*.*
cpe:2.3:o:canonical:ubuntu_linux:18.10.*.*.*.*.*.*
cpe:2.3:o:debian:debian_linux:8.0.*.*.*.*.*.*
cpe:2.3:o:debian:debian_linux:9.0.*.*.*.*.*.*
cpe:2.3:o:debian:debian_linux:8.0.*.*.*.*.*.*
cpe:2.3:o:debian:debian_linux:9.0.*.*.*.*.*.*
cpe:2.3:o:oracle:linux:7.0.*.*.*.*.*.*
cpe:2.3:o:oracle:linux:7.0.*.*.*.*.*.*
cpe:2.3:a:qemu:qemu:2.1.0.*.*.*.*.*.*
cpe:2.3:a:qemu:qemu:2.12.0.*.*.*.*.*.*
cpe:2.3:a:qemu:qemu:2.8.0.*.*.*.*.*.*
cpe:2.3:a:qemu:qemu:2.1.0.*.*.*.*.*.*
cpe:2.3:a:qemu:qemu:2.12.0.*.*.*.*.*.*
cpe:2.3:a:qemu:qemu:2.8.0.*.*.*.*.*.*
cpe:2.3:o:redhat:linux:6.0.*.*.*.*.*.*
cpe:2.3:o:redhat:linux:6.0.*.*.*.*.*.*
cpe:2.3:o:suse:linux_enterprise_server:11:sp3.*.*:ltss.*.*.*
cpe:2.3:o:suse:linux_enterprise_server:11:sp4.*.*.*.*.*.*
cpe:2.3:o:suse:linux_enterprise_server:12.*.*.*:ltss.*.*.*
cpe:2.3:o:suse:linux_enterprise_server:15.*.*.*.*.*.*
cpe:2.3:o:suse:linux_enterprise_server:11:sp3.*.*:ltss.*.*.*
cpe:2.3:o:suse:linux_enterprise_server:11:sp4.*.*.*.*.*.*
cpe:2.3:o:suse:linux_enterprise_server:12.*.*.*:ltss.*.*.*
cpe:2.3:o:suse:linux_enterprise_server:15.*.*.*.*.*.*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023   |

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](#)