



CVE-2018-14625

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

Last Modified on: 02/13/2023 04:51:00 AM UTC

CVE-2018-14625

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

CVSS:30/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H



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

A flaw was found in the Linux Kernel where an attacker may be able to have an uncontrolled read to kernel-memory from within a vm guest. A race condition between connect() and close() function may allow an attacker using the AF_VSOCK protocol to gather a 4 byte information leak or possibly intercept or corrupt AF_VSOCK messages destined to

other clients.

CVE-2018-14625 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **[UNKNOWN]** - kernel version = n/a

CVSS3 Score: **7 - HIGH**

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

CVSS2 Score: **4.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

USN-3871-3: Linux kernel (AWS, GCP, KVM, OEM, Raspberry Pi 2) vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3871-3
KASAN: use-after-free Read in vhost_transport_send_pkt	Third Party Advisory syzkaller.appspot.com text/html	 MISC syzkaller.appspot.com/bug?extid=bd391451452fb0b93039
CVE-2018-14625 - Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2018-14625
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:2029
USN-3872-1: Linux kernel (HWE) vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3872-1
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:2043
1619846 – (CVE-2018-14625) CVE-2018-14625 kernel: use-after-free Read in vhost_transport_send_pkt	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=1619846
USN-3871-5: Linux kernel (Azure) vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3871-5
[SECURITY] [DLA 1771-1] linux-4.9 security update	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20190503 [SECURITY] [DLA 1771-1] linux-4.9 security update
1619846 – (CVE-2018-14625) CVE-2018-14625 kernel: use-after-free Read in vhost_transport_send_pkt	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-14625
USN-3871-4: Linux kernel (HWE) vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3871-4
USN-3878-2: Linux kernel (Azure) vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3878-2
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:4154
USN-3871-1: Linux kernel vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3871-1
USN-3878-1: Linux kernel vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3878-1

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	8.0	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
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: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:8.0:***:***:***:						
cpe:2.3:o:linux:linux_kernel:-:***:***:***:						

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:

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](#)